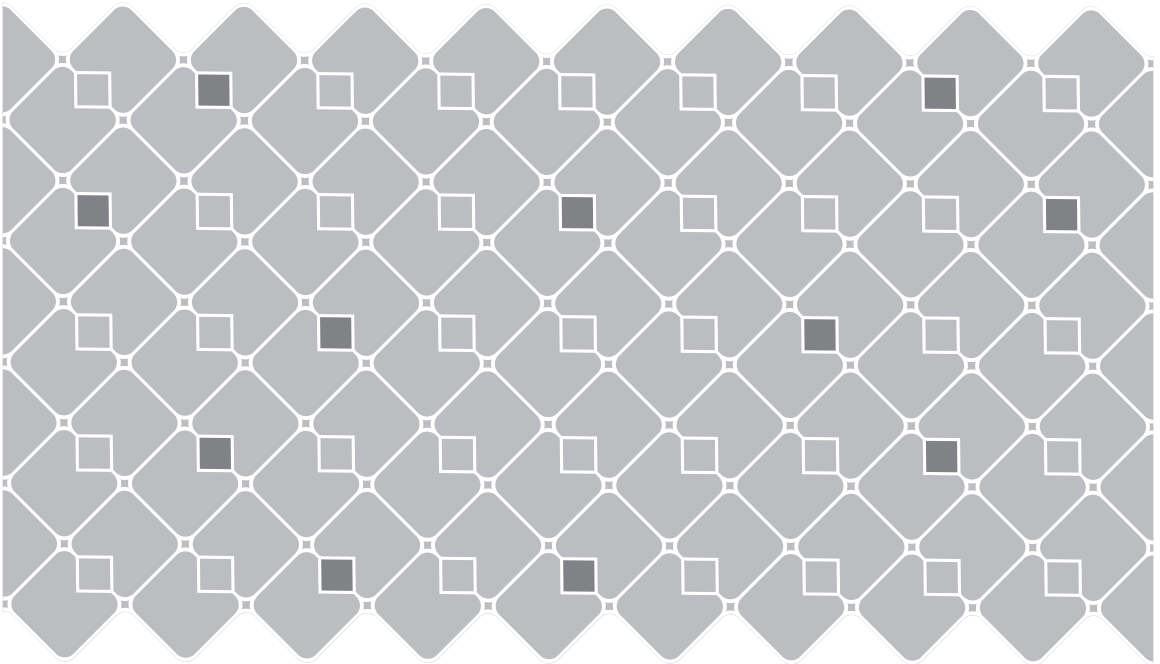
VMware ACE Management Server User's Manual

VMware ACE 2.5



vmware®

VMware ACE Management Server User's Manual
Revision: 20071019
Item: ACE-ENG-Q207-008

You can find the most up-to-date technical documentation on our Web site at

http://www.vmware.com/support/

The VMware Web site also provides the latest product updates.

If you have comments about this documentation, submit your feedback to:

docfeedback@vmware.com

Beta

© 2004-2008 VMware, Inc. All rights reserved. Protected by one or more of U.S. Patent Nos. 6,397,242, 6,496,847, 6,704,925, 6,711,672, 6,725,289, 6,735,601, 6,785,886, 6,789,156, 6,795,966, 6,880,022, 6,944,699, 6,961,806, 6,961,941, 7,069,413, 7,082,598, 7,089,377, 7,111,086, 7,111,145, 7,117,481, 7,149,843, 7,155,558, 7,222,221, 7,260,815, 7,260,820, 7,269,683, 7,275,136, 7,277,998, 7,277,999, 7,278,030, 7,281,102, and 7,290,253; patents pending.

VMware, the VMware "boxes" logo and design, Virtual SMP and VMotion are registered trademarks or trademarks of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

VMware VirtualCenter 2.5 is distributed with certain third party technology licensed from Tom Sawyer Software. Tom Sawyer Visualization (c) 2004 Tom Sawyer Software, Oakland, California. All Rights Reserved.

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

About This Book 7

1 Introduction 9
- System Requirements 9
  - Hardware 9
  - Software 10
  - External Databases 10
  - Web Browsers 10
  - Licensing 10

2 ACE Management Server Deployment 11
- Deploying ACE Management Server 11
- Performing Capacity Planning 12
  - Deployment Platforms 12
  - Scalability Factors 13
  - Clients Supported for Each Server 13
- Database Throughput and Scalability 13
  - LDAP Throughput 14
  - Network Bandwidth 14
  - ACE Policy Configuration 15
- Deploying Thousands of Clients 16
- Security 16
- Access from Outside the Corporate Firewall 17

3 Installing and Configuring ACE Management Server 19
- Features of ACE Management Server 20
- ACE Management Server Setup Options 21
- Configuring TLS in Your Browser 22
- ACE Management Server Components 23
  - Database Options 23
    - Database Backup 24
- Installing ACE Management Server 25
  - Default Port Assignments for ACE Management Server 26

Beta

Installing ACE Management Server on a Windows System 26
Installing ACE Management Server on a Linux System 26
Using SSL Certification and Protocol 30
Setting Up Custom Certificates 31
Configuring Multiple ACE Management Servers to Use SSL 33
Configuring ACE Management Server 34
Prerequisites for Configuring the Server 34
Obtain Your ACE Management Server License Information 34
Using Active Directory Integration by using LDAP 34
Using an External Database 35
Performance Optimization Tips for External Database Use 38
Using an External Database with the ACE Management Server Appliance 39
Using the ACE Management Server Setup Application 40
Deleting the ACE Management Server Configuration File and Setting a New Administrator Password 43
Using Event Logs 46
Stopping and Starting the Apache Service Manually 46
Logging In to ACE Management Server 47
Using ACE Management Server 48
Connection Problems Between a Linux ACE Instance and ACE Management Server 48
Change the Port Assignment for ACE Management Server 48
Using the VMware Help Desk Web Application 49
Managing Instances 50

4 Instance Management 55
Viewing All Instances that a Server Manages 56
Searching for Instances 56
Managing Columns in the Instance View Table 58
Managing Custom Columns 58
Viewing General Statistics 60
Resetting the Password and Copy Protection ID on the Policies Tab 61
Creating Custom Columns 61

A Database Schema and Audit Event Log Data 63
Database Schema 63
Querying the Audit Event Log Data 68

Beta

Glossary 73

Index 79

Beta

Beta

About This Book

This manual, the *VMware ACE Administrator's Manual*, provides information about installing and using Workstation.

Intended Audience

This book is intended for anyone who needs to install, upgrade, or use Workstation with ACE enabled. ACE users typically include people who do software development and testing or work with multiple operating systems or computing environments: software developers, QA engineers, trainers, salespeople who run demos, and anyone who wants to create virtual machines.

Document Feedback

VMware welcomes your suggestions for improving our documentation. If you have comments, send your feedback to:

docfeedback@vmware.com

Technical Support and Education Resources

The following sections describe the technical support resources available to you.

Self-Service Support

Use the VMware Technology Network (VMTN) for self-help tools and technical information:

- Product information – http://www.vmware.com/products/

Beta

- Technology information – http://www.vmware.com/communities/content/
- Documentation – http://www.vmware.com/support/pubs
- VMTN Knowledge Base – http://kb.vmware.com
- Discussion forums – http://www.vmware.com/community
- User groups – http://www.vmware.com/communities/content/vmug/

For more information about the VMware Technology Network, go to http://www.vmware.com/community/index.jspa.

Online and Telephone Support

Use online support to submit technical support requests, view your product and contract information, and register your products. Go to http://www.vmware.com/support.

Customers with appropriate support contracts should use telephone support for the fastest response on priority 1 issues. Go to http://www.vmware.com/support/phone_support.html.

Support Offerings

Find out how VMware support offerings can help meet your business needs. Go to http://www.vmware.com/support/services.

VMware Education Services

VMware courses offer extensive hands-on labs, case study examples, and course materials designed to be used as on-the-job reference tools. For more information about VMware Education Services, go to http://mylearn1.vmware.com/mgrreg/index.cfm.

Beta

Introduction 1

The VMware® ACE Management Server enables you to manage VMware ACE instances, to dynamically publish policy changes for those instances, and to test and deploy packages more easily. It adds new integration with your Active Directory setups and provides secure Active Directory-LDAP integration, with role-based secure SSL communication.

This chapter discusses the following topics:

"System Requirements" on page 9

System Requirements

The following sections describe the ACE Management Server system requirements.

Hardware

- A minimum of an 800MHz-compatible x86 and x86-64 architecture processor

  Compatible processors include:

  Celeron, Pentium II, Pentium III, Pentium 4, Pentium M (including computers with Centrino mobile technology), Xeon (including Prestonia), AMD, Athlon, Athlon MP, Athlon XP, Duron, Opteron, AMD64 Opteron, Athlon 64

- Experimental support for Intel IA-32e CPU
- 40MB of free space is required for basic installation. VMware recommends at least 10GB of free disk space.
- An 8-bit display adapter is required.

Beta

- For local area networking, any Ethernet controller that the operating system supports is sufficient.

Software

- Windows Server 2003 Web Edition SP1, SP2, Windows Server 2003 Standard Edition SP1, SP2, Windows Server 2003 Enterprise Edition SP1, SP2 (includes 64-bit and R2 editions)
- Windows XP Professional (includes 64-bit editions)
- Windows 2000 Server Service Pack 4, Windows 2000 Advanced Server Service Pack 4
- Red Hat Enterprise Linux Advanced Server 4.0 with Update 4.
- SUSE Linux Enterprise Server 9 Service Pack 3

External Databases

The SQLite database engine is embedded in the ACE Management Server.

In addition, you can use external databases through ODBC connectivity:

- **Windows-based servers** – Microsoft SQL Server 2000 or later; Oracle Database 10*g*
- **Linux-based servers** – PostgreSQL 7.4 or later; Red Hat Enterprise Linux Advanced Server 4.5 or later.

Web Browsers

ACE Management Server configuration and ACE Management Server Help Desk Web application requires one of the following Web browsers:

- Mozilla Firefox 1.52 or later
- Internet Explorer 6.0 or later

Licensing

You must configure the server and enter the license in the server setup Web application. If you do not, you cannot connect to the server in Workstation. Workstation and ACE instances cannot connect to an ACE Server with an expired or nonexistent license.

Beta

ACE Management Server Deployment 2

Beta

This chapter provides guidelines for deploying VMware ACE Management Servers, including capacity planning and best practices. This chapter discusses the following topics:

- "Deploying ACE Management Server" on page 11
- "Performing Capacity Planning" on page 12
- "Database Throughput and Scalability" on page 13
- "Deploying Thousands of Clients" on page 16
- "Security" on page 16
- "Access from Outside the Corporate Firewall" on page 17

Deploying ACE Management Server

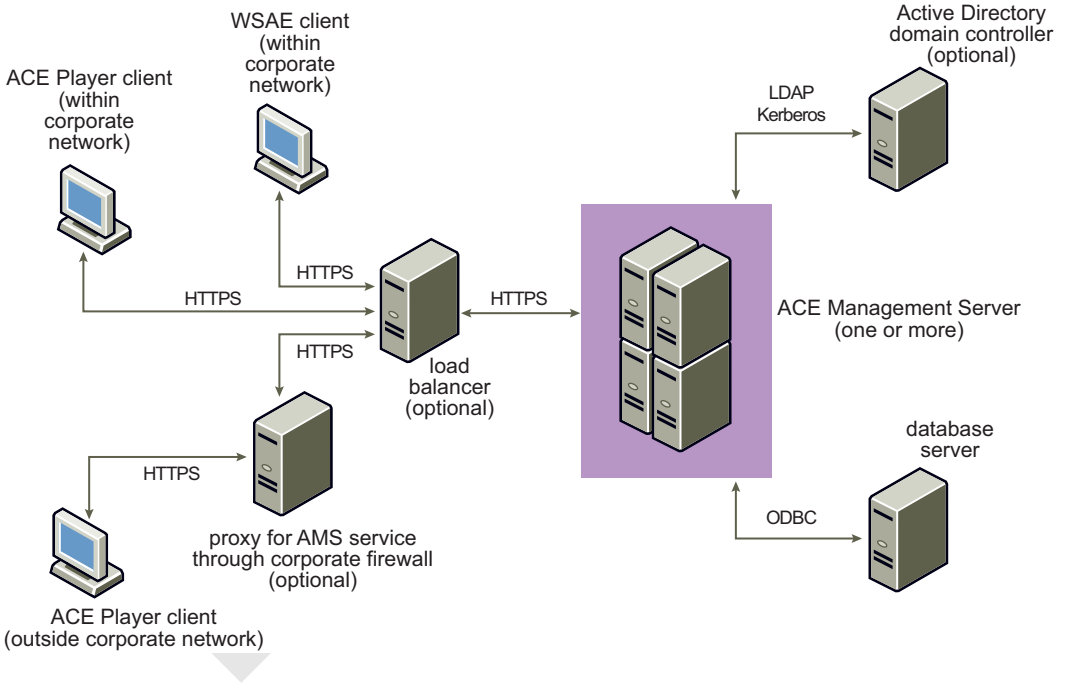
A typical ACE Management Server deployment has the following components:

- **One or more ACE Management Servers –** You can configure multiple servers to work on the same database and increase the capacity of your service. You can also deploy multiple servers for high availability.
- **(Optional) HTTP load balancer –** Use a load balancer to help scale the capacity of your ACE Management Server deployment.
- **Database server –** For production deployments, VMware recommends Oracle or MS-SQL (Windows ACE Management Server), and Postgres (Linux ACE Management Server).

- **(Optional) Active Directory domain controller** – To enable the ACE Management Server Active Directory integration, you must configure ACE Management Server to communicate with your domain controller.

For an example of an ACE Management Server deployment, see Figure 1.

Figure 1. Comprehensive ACE Management Server Deployment



Performing Capacity Planning

ACE Management Server enables you to manage ACE instances and policies in real time. Capacity planning is important because every ACE instance deployed in your enterprise might need to communicate with your ACE Management Servers.

Deployment Platforms

Choose from the following platforms to deploy ACE Management Server:

- Windows 2003 Server
- VMware Virtual Appliance
- RHEL 4

- SUSE Linux Enterprise Server 9

The platforms differ in the libraries they use to connect to active directory and the external databases they support.

Scalability Factors

The number of clients that a single ACE Management Server installation can serve depends on several key factors:

- Database throughput and scalability
- LDAP throughput (if you are using Active Directory)
- Network bandwidth available for incoming client requests
- Policy update frequency for your deployed instances
- ACE policy configuration

Clients Supported for Each Server

Table 1 lists recommendations for the number of clients supported based on the platform you are using. The figures shown reserve some server processing power so that interactive clients receive responses in a timely fashion and increases in demand are satisfied by the server.

Table 1. Number of Clients Supported

Platform	Recommended Clients
GHz AMD 2-way server (Opteron 280, 4GB RAM)	6,000
GHz Intel 2-way desktop machine (4GB RAM)	4,000

Database Throughput and Scalability

For production deployments, VMware recommends that you use Oracle, MS-SQL, or Postgres as your database platform.

Over 95% of the storage space that ACE Management Server requires is used to log event information, which is an audit trail of all transactions performed through ACE Management Server.Table 2 lists recommended database sizes based on the number of clients being served.

The figures in the table are based on a 90-day database archival period. Store your database records every 90 days and keep event logs for up to 90 days.

Beta

Table 2. Database Storage Recommendations

Number of Clients	Recommended Database Size
100	50Mb
1,000	500Mb
10,000	5,000Mb

You can configure your ACE Management Server to purge event logs every 90 days.

You can configure ACE Management Server to log less event information. From the ACE Management Server web configuration page, click the **Logging** tab. The authentication event generates most of the data because an event is generated every time someone attempts to authenticate to ACE Management Server.

LDAP Throughput

ACE Management Server communicates with your Active Directory domain controller to authenticate user credentials. Your domain controller infrastructure handles the LDAP traffic required to support the number of clients that you anticipate.

Integrating with Active Directory through LDAP is implemented differently in the Windows ACE Management Server than in the Linux-based ACE Management Server. The Windows ACE Management Server uses the WinLDAP library bundled with your Windows Operating System. The Linux ACE Management Server uses a third-party Kerberos Library and OpenSSL. Internal testing results indicate that the Windows implementation is superior in both performance and configuration.

When configuring ACE Management Server to use LDAP, follow these guidelines to avoid affecting performance:

- The host name for the LDAP host must be fully qualified (for example, `ldap.vmware.com`) instead of an IP address or host name with no domain postfix.
- The default domain is the domain for which the LDAP host is a domain controller.
- The query user is a user in the default domain.
- The admin user group is a group that exists in the default domain.

Network Bandwidth

The amount of network bandwidth that ACE Management Server and ACE instances require depends on the frequency of policy updates that you have configured. Table 3 shows the amount of bandwidth needed when you use a policy update frequency value of 10 minutes.

Beta

Table 3. Network Bandwidth Required with a Policy Update Frequency of 10 Minutes

Number of Clients	Bandwidth Required
100	0.125 Mb/sec
1,000	1.25 Mb/sec
10,000	12.5 Mb/sec

VMware recommends that you increase the time between policy updates by clients for large deployments (more than 5,000 clients) because this reduces the amount of required bandwidth.

If you modify your policy update frequency, you can increase or decrease your network bandwidth requirements. For example, if you change the value to 30 minutes it requires one third as much bandwidth for the same number of clients.

Table 4 shows the bandwidth when the policy update frequency value is set to 30 minutes.

Table 4. Network Bandwidth Required with a Policy Update Frequency of 30 Minutes

Number of Clients	Bandwidth Required
100	0.04 Mb/sec
1,000	0.4 Mb/sec
10,000	4 Mb/sec

The amount of network bandwidth required could also be higher if your policy set is very complex.

VMware recommends that you have a separate network link between ACE Management Server and your database server, so that traffic coming and going from ACE Management Server to its clients does not interfere with the traffic to and from your database server.

ACE Policy Configuration

The configuration of ACE policies can affect performance. You can increase the amount of data that is transferred between ACE Management Server and ACE Player by using one of the following methods:

- **Host policies** – Enabling host policies (such as host network quarantine) requires that a host-side daemon retrieve the host policies from ACE Management Server.

Beta

- **Complex network quarantine policies** – If the set of rules that makes up your network quarantine is very large, the transfer of these rules from ACE Management Server to the clients can affect the scalability.

  The numbers shown in Table 3 and Table 4 are estimates of required bandwidth given average-size rule sets for network quarantine. You can view the size of your policy set by examining the ACE file directory and counting the size of the `.vmpl` file. An average policy set is 15KB or less.

Deploying Thousands of Clients

The ACE Management Server client-server protocol is built on top of the HTTPS protocol. You can use HTTP load-balancing software and hardware solutions to scale an ACE Management Server deployment beyond the capacity of a single server (or for high-availability deployments).

ACE Management Server scales in a linear fashion when an enterprise grade HTTPS load balancer is used. See the *Configuring Multiple ACE Management Servers* technical note.

Security

Use the following recommendations to configure ACE Management Server to minimize security problems:

- **Traffic to and from clients is protected by HTTPS** – By default, ACE Management Server creates a self-signed certificate when you install it to use for HTTPS traffic. These certificates are secure, but you can also configure ACE Management Server to use your own certificate and key pairs.
- **Traffic from ACE Management Server to Active Directory is encrypted** – LDAP traffic is encrypted at the application layer. Credentials are protected by using the Kerberos protocol to authenticate credentials.
- **Sensitive configuration options are encrypted** – Passwords stored in the configuration file are encrypted.
- **Database Security** – The database store contains sensitive data such as cryptographic keys. Configure your database security so that it is protected from intrusion and protected in case of data loss. (For more information about features that are available to protect your data, see your database documentation.)

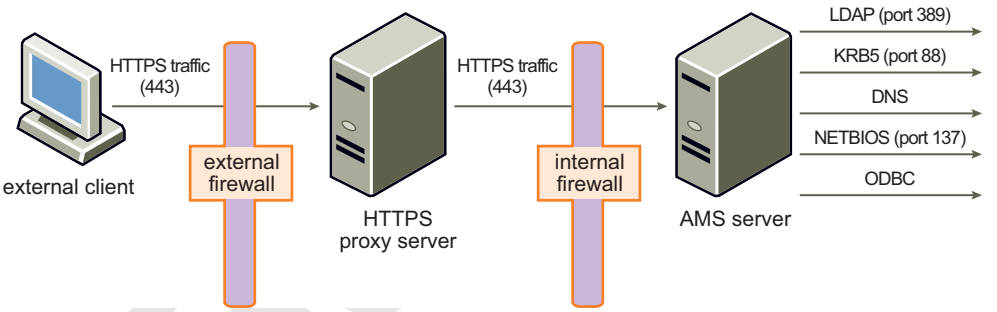
Beta

Access from Outside the Corporate Firewall

All client requests to ACE Management Server are HTTPS traffic on port 443. This means that any solution using a proxy to secure HTTPS traffic into your corporate servers can be used to proxy ACE Management Server traffic.

VMware recommends the use of an HTTPS proxy in the DMZ, which relays ACE Management Server traffic to the actual ACE Management Server inside the corporate network. Because of the number of data connections that the ACE Management Server must make on the back end (LDAP, DNS, ODBC, KERBEROS), VMware recommends this deployment strategy.

Figure 2. Recommended Deployment for External Access to ACE Management Server



ACE Management Server uses the following data connections:

- LDAP – Port 389, LDAP queries are encrypted.
- Kerberos – Port 88.
- DNS
- ODBC – See the ODBC documentation on your server platform for information on how to secure ODBC traffic.
- NETBIOS – Port 137.

ACE Management Server can be deployed with the following HTTPS proxy solutions:

- Apache Proxy – Using `mod_proxy`
- Zeus Technology Load Balancer – A commercially available load balancer and traffic management solution.

Avoid the following problems when you use a proxy for traffic into ACE Management Server:

- **SSL Termination** – If your HTTPS proxy terminates the SSL connection, you must use the same SSL key and certificate on the HTTPS proxy server and ACE Management Server. Or, use the ACE Management Server certificate chain to embed the HTTPS proxy certificate verification chain in the ACE package.

  An example of a proxy server that terminates SSL connections is Apache Proxy. The Zeus load-balancing products support SSL passthrough, which means that the SSL connection is terminated at ACE Management Server.

- **Multiple ACE Management Server SSL certificates** – If you are deploying multiple ACE Management Servers behind a load-balancing solution, all ACE Management Servers must use the same SSL key and certificate pair. You can also use the ACE Management Server certificate chain feature to embed every SSL certificate verification chain into the ACE package).

- **DNS resolution** – When you create an ACE Master, you must specify a host name for ACE Management Server. This host name must resolve to the appropriate IP address for both internal and external clients. Internally, it can resolve to ACE Management Server itself. Externally, it can resolve to the HTTPS proxy server.

Because the traffic coming into ACE Management Server is plain HTTPS traffic and the server is stateless, many other configurations can be deployed to provide external access to ACE Management Server. When you design your deployment, think of ACE Management Server as a regular web server with secure traffic.

Beta

Installing and Configuring ACE Management Server

3

Beta

VMware ACE Management Server enables you to manage ACE instances in real time. Including ACE Management Server in your system setup enables you to do the following:

- Manage activation of ACE packages.
- Manage authentication of those activated packages.
- Dynamically deliver policy updates to managed ACE instances.
- Dynamically deliver instance customization data for managed ACE instances with Windows guest operating systems.

NOTE Using ACE Management Server is optional.

The following topics are covered in this chapter:

- "Features of ACE Management Server" on page 20
- "ACE Management Server Setup Options" on page 21
- "Configuring TLS in Your Browser" on page 22
- "ACE Management Server Components " on page 23
- "Installing ACE Management Server" on page 25
- "Using SSL Certification and Protocol" on page 30
- "Configuring ACE Management Server" on page 34
- "Using Event Logs" on page 46
- "Stopping and Starting the Apache Service Manually" on page 46

- "Logging In to ACE Management Server" on page 47
- "Using ACE Management Server" on page 48

Features of ACE Management Server

ACE Management Server has the following features:

- Scalability and reliability:
  - You can increase capacity by adding network resources such as load balancers and extra server hardware.
  - For single-server small-size to medium-size deployments, the default embedded backing store provides a simple and efficient database solution. To scale ACE Management Server for large deployments, you can configure and use an external RDBMS.
  - Server requests are handled by multithreaded processes with the Windows operating system and by multiple processes in Linux operating systems. If one process dies, another takes over.
- Active directory integration:
  - You can use Active Directory to authenticate users of ACE instances.
  - No schema change for your existing Active Directory is required.
  - LDAP is used to access Active Directory.
  - Information about Windows domain user account states is provided in clear and useful messages. Reasons for login failures are presented as "locked out" or "password expired."
  - ACE Management Server acts as an Active Directory password change proxy.
  - You can use the instance customization feature in ACE with your own established naming conventions to associate users with machines.
- Security:
  - Communications are SSL-encrypted. Communications between server and clients, over HTTPS traffic.
  - Passwords are stored securely in hashed form in the backing store.

  Flexible database options allow use of an embedded database or external relational database management systems to store ACE instance data and policies.

- Simple installation and configuration:
  - The server uses off-the-shelf software components:
    - Apache Web server 2.0
    - The default SQLite database store
  - The server setup uses industry-standard protocols:
    - HTTPS and LDAP
    - xml-rpc for message encapsulation
  - Client traffic can be proxied by off-the-shelf products.
  - The Windows installer for Workstation includes the installation components for ACE Management Server.
- Extensibility and availability:
  - You can create and use more than one ACE Management Server. When you use more than one server, you can set the servers up so that they share the same database for load balancing or increased fault tolerance. To use increased fault tolerance, you use an external database. If your multiple servers do not need to share a database (the servers are independent of one another), you can use either the embedded database or an external RDBMS.
  - A Windows system ACE Management Server can be on the same system as Workstation.
  - You can designate a single ACE Management Server name, such as `https://ace.policyserver.company.com`, and use DNS lookup to translate the host name into an address. The address is cached if a DNS server is not available. Additionally, different ACE Management Servers can be used if users travel between offices in different geographic locations.

    NOTE Your server name must be either the machine name in English or the IP address. International characters are not supported.

Related Topics

- "Database Options" on page 23

ACE Management Server Setup Options

The clock on the host system that has ACE 2 Management Server installed or running the ACE 2 Management server appliance must be synchronized with the client system. Use Network Time Protocol (NTP) to synchronize the clocks.

To set up an ACE Management Server, choose one of the following options:

- Install the server on a Windows host system.
- Install the server on a Linux host system.
- Download and configure the ACE Management Server appliance.

If you set up multiple ACE Management Servers, they must all be the same type.

You can download the ACE Management Server appliance from the ACE 2 page and configure it as your ACE Management Server.

The ACE Management Server appliance is a self-contained, preinstalled, and preconfigured ACE Management Server packaged with a small operating system in a virtual machine.

By default, the appliance attempts to configure its network by using DHCP. You can optionally configure the network settings yourself, using the supplied ACE Management Server Appliance Configuration and Management Web interface. You can use that same interface to update the appliance when updates become available.

You must have access to a Web browser (Mozilla 1.52 or later or Internet Explorer 6.0 or later) to change network settings or obtain updates for the appliance.

Configuring TLS in Your Browser

TLS must be configured on your Web browser to operate ACE Management Server.

To configure TLS in an Internet Explorer browser

1 Choose **Tools > Internet Options > Advanced** and scroll down to **Securit**y.

2 Select **Use TLS 1.0** check box and click **OK**.

To configure TLS in a Mozilla browser

1 Choose **Tools > Options > Advanced.**

2 Select **Use TLS 1.0** and click **OK**.

Related Topics

- "Windows Server 2003 Web Edition SP1, SP2, Windows Server 2003 Standard Edition SP1, SP2, Windows Server 2003 Enterprise Edition SP1, SP2 (includes 64-bit and R2 editions)" on page 10
- "Red Hat Enterprise Linux Advanced Server 4.0 with Update 4." on page 10
- "To install the ACE Management Server appliance" on page 28

ACE Management Server Components

ACE Management Server has the following components:

- Platform, based on the Apache 2.0 web server
- Backing store technology, the database layer for the server component
- Active Directory integration:
  - Permits joining an operating system that is running an ACE instance to the domain remotely.
  - Provides search functions so you can quickly find a particular individual or group.
  - Enables you to use Active Directory Users and Groups to configure role-based access to the features of ACE Management Server.
- SSL certificate management
- Event logging

Database Options

ACE Management Server offers the following database options:

- **Embedded SQLite database –** The default mode of ACE Management Server works with an embedded SQLite 3 database engine. The SQLite database engine is initialized during server installation and requires no special configuration. The embedded database supports up to several gigabytes of data.
- **Supported external database –** If your enterprise IT environment requires the reliability and performance characteristics of a commercial database engine, you can use a supported external database as a backing store for ACE Management Server, through ODBC connectivity. Supported external database engines are Microsoft SQL Server (SQL Server 2000 or SQL Server 2005) and Oracle Database 10g for Windows-based servers and PostgreSQL 7.4 or higher for Linux-based servers.

  NOTE If ACE Management Server is deployed in the DMZ, use an external database located inside your corporate network behind a firewall.

  Using an external database with ACE Management Server offers these benefits:

  - Online backup – You do not have to shut down ACE Management Server to back up the database.

- Enhanced security model – You can fine-tune permissions to access sensitive data. The SQLite database engine provides file-system based security.
- Performance fine-tuning
- Ability to use external database management and reporting tools.

If your setup includes load-balanced ACE Management Servers, you must use an external RDBMS as the backing store, because the SQLite database cannot be shared across processes running on multiple machines.

NOTE The SQLite database is file based and is not designed to be effectively shared across multiple processes. If you use third-party tools to access the database for a read operation, therefore, you cannot depend on transactional isolation of the pending write operations of the ASM.

Database Backup

If you are using an external database, you can use the backup and recovery strategy that you have determined is appropriate for your database system.

CAUTION Back up your ACE Management Server database on a regular basis to ensure that the database can be recovered promptly if needed.

If you are using the embedded database, you can use standard file-backup tools, such as `ntbackup` or `dd`. The data is stored in one of the following locations:

- **Windows** – `C:\Program Files\VMware\VMware ACE Management Server\db\acesc.bin`.
- **Linux** – `/var/lib/vmware/acesc/db/acesc.bin`

If you are using the embedded database in a production environment, stop the server, copy the file to a different location for the backup, and restart the server. SQLite is file based, so the database file might be modified by the ACE Management Server process at the same time that it is being copied for backup, meaning that an inconsistent database snapshot might be produced. This problem is unlikely to occur because the file is usually not large and is copied quickly.

Other alternatives for backing up an open database, as recommended by members of an SQLite community, as discussed in this forum thread, are noted below:

http://marc.10east.com/?l=sqlite-users&m=111487876701133&w=2

- Log in to the SQLite database using the `sqlite3` command-line tool. Use the `.dump` command, store the result in a separate file, and back up that result file. It is a SQL script that will recreate the database.

- Using the Shadow Volume Copy mechanism on Windows systems or LVM volume snapshots on Linux (and the crash-restore feature of SQLite), back up the complete database directory, including journal files if they are present. This method is actually easier than it sounds: On a Windows XP SP1 or later operating system, just use `ntbackup` on the database directory. When the database is restored it should work fine.
- Log in to the database as described in the first method. Issue BEGIN EXCLUSIVE, copy the database file, and then issue COMMIT.

For information about using your company's own management or reporting tools or automated scripts with the data in the VRM database, see "Database Schema and Audit Event Log Data."

Related Topics

- "Using SSL Certification and Protocol" on page 30
- "Using Event Logs" on page 46

Installing ACE Management Server

Before you can create a managed ACE-enabled virtual machine, you must have an ACE 2 Management Server set up and configured.

Target hardware platform support for ACE Management Server depends almost exclusively on the number of ACE instances being supported and the frequency with which they are configured to communicate with the server. VMware recommends that production deployments be installed on either a dedicated server or a virtual platform with sufficient available resources to ensure performance and stability. For more information about VMware performance testing, see the sizing white paper.However, ACE Management Server was tested and can be installed on desktop or workstation platforms to support a small number of clients or nonproduction evaluations.

Topics in this section are:

- "Default Port Assignments for ACE Management Server" on page 26
- "Installing ACE Management Server on a Windows System" on page 26
- "Installing ACE Management Server on a Windows System" on page 26
- "Installing ACE Management Server on a Linux System" on page 26
- "To install the ACE Management Server appliance" on page 28

Default Port Assignments for ACE Management Server

Table 3-1 lists the default port assignments for ACE Management Server.

Table 3-1. Port Assignments, Default Settings, for ACE Management Server

Port	Used For:
https port 443	Communications between ACE Management Server and ACE instances
https port 8000	ACE Management Server Setup (configuration) Web application
	ACE Help Desk Web application
https port 8080	ACE Management Server Appliance configuration

NOTE If another Web server is installed that uses any of these default ports, you might need to resolve the conflict.

Installing ACE Management Server on a Windows System

Install ACE Management Server by launching the `vmware-ace-management-server` application from the server on which ACE Management Server will reside. The `vmware-ace-management-server.exe` file is available as a separate downloadable file in the same download location as the Workstation application.

To install the server, follow the prompts in the installation wizard.

If you are installing the server on a host computer that has a firewall enabled, you might see a message at the end of the installation asking whether you want to unblock the Apache service. Choose **Unblock**. ACE Management Server does not work properly if you do not unblock the service.

CAUTION On the Server Information page in the wizard, ensure that the server name you use matches the name of the machine on which you are installing ACE Management Server. If you set the server name to something other than this, you cannot log in to ACE Management Server after you finish the installation and ACE instances might have trouble making required connections to the server during activation.

Installing ACE Management Server on a Linux System

You can install ACE Management Server on the following Linux systems:

- Red Hat Enterprise Linux 4
- SUSE Linux Enterprise Server 9 SP3

Before you install ACE Management Server on a Linux system, you must meet these requirements:

- A working installation of Apache 2.0 is installed on the system. (The RPM for a Web server comes with your RHEL4 or SUSE Linux Enterprise Server 9 installation.)
- Apache Web service is operating normally and is receiving requests for SSL http.
- The `mod_ldap` and `mod_ssl` modules are available on your system.
- The following packages are installed on your RHEL4 or SUSE Linux Enterprise Server 9 system:

  `curl, openldap, openssl, apache, gdbm`
- For SUSE Linux Enterprise Server 9, install the `cyrus-sasl-gssapi` package. This package is not installed by default.
- When you use the external database option, the following packages are required as well:
  - RHEL4: `unixODBC`
  - SUSE Linux Enterprise Server 9: `unixODBC` and, if you plan to use the X11 graphical configuration tool, `unixODBC-gui-qt`

To install ACE Management Server on a Red Hat Enterprise Linux 4 or SUSE Linux Enterprise Server 9 system

1 Run the appropriate `rpm` installer for ACE Management Server:

```
vmware-ace-management-server-<build_number>.i386-rhel4.rpm
vmware-ace-management-server-<build_number>.i386-sles9.rpm
```

2 For an SUSE Linux Enterprise Server 9 server, ensure that the LDAP module (`mod_ldap`) is configured for loading:

   a Open the following file with a text editor:

   `/etc/sysconfig/apache2`

   b Add the `ldap` config option to the `APACHE_MODULES` variable.

   c Save and close the file.

To install the ACE Management Server appliance

1 Download the zipped file for the appliance from the ACE 2 release download page:

`VMware-ACE-Management-Server-Appliance-2.0.0-<NNNNN>.zip`

<NNNNN> is the ACE build number.

2 Extract the zipped files to the directory where the server is to be located.

3 Start VMware Workstation and choose **File > Open** to open and run `ams_appliance.vmx`.

4 At the password prompt, enter a password and confirm it.

This password is used for both root and network accounts. Make a note of this password so that you can use it for later appliance management operations from the console and the Web.

The appliance configures its network by using DHCP.

The console view displays the following information:

- The current network settings
- The URLs for remotely administering the appliance and configuring the ACE Management Server itself:

For the Appliance Management and Configuration application:

`https://<hostIPaddress>:8080/`

For the ACE Management Server Setup application:

`https://<hostIPaddress>:8000/`

This information appears above each login prompt. If you press **Return** at the login prompt, the information is displayed again.

5 At the time zone prompt, accept the current setting or make a change as needed.

6 (Optional) To reconfigure the network—for instance, to configure the server to use a static IP address or to specify a proxy server, reconfigure the network settings from the current console view by following the prompts and instructions on the screen.

You can also reconfigure the network settings by using the Appliance Management and Configuration application, as follows:

a Leave the ACE Management Server appliance running.

b Browse to:

```
https://<hostIPaddress>:8080/
```

c In the connection dialog box, type **root** in the user name field and your network or root password in the password field.

d Click the **Network** link on the first page of the Appliance Configuration and Management Web application to open the Network Configuration page.

e To view instructions about configuring network settings, click the **Help** link in the upper right of the Web page.

f After you've made the changes you want to make to the network settings, click **Apply**. To revert to the settings that were on the page before you started making changes, click **Reset**.

7 (Optional) To reconfigure any update options, for example, to disable automatic downloads of updates, use the Appliance Management and Configuration application, as follows:

a Leave the ACE Management Server appliance running.

b Browse to:

```
https://<hostIPaddress>:8080/
```

c In the connection dialog box, type "**root**" in the user name field and your network/root password in the password field.

d Click the **Update** link on the first page of the Appliance Configuration and Management Web application to open the Appliance Update page.

e To view instructions about configuring update options, click the **Help** link in the upper right of the Web page.

8 When you have finished configuring any network or update settings, navigate to the ACE Management Server Setup Web application to configure the server.

To access that application, choose one of these methods:

- From the Appliance Management and Configuration Web application page, click the **ACE Login** link at the top right of the page.
- Browse to the ACE Management Server Setup Web application:

```
https://<hostIPaddress>:8000/
```

9 Click **Configuration** to open the Web application.

Using SSL Certification and Protocol

By default, ACE Management Server uses the Secure Sockets Layer (SSL) protocol to provide encrypted, secure communications. The server connects to its managed instances using SSL. If the server is integrated with an Active Directory service, it communicates with the service through an SSL-protected link.

SSL encrypts data through the use of a public-key/private-key pair. The public key is known to everyone and the private key is known only to the message recipient. URLs that require an SSL connection start with https.

ACE Management Server must be configured to use SSL. For more information on configuring ACE Management Server to use SSL, see "Configuring Multiple ACE Management Servers to Use SSL" on page 33.

The following is a description of how ACE Management Server uses SSL.

At ACE Management Server installation, the following two files are created:

- server.key – An RSA 1024-bit key, this is the private key.
- server.crt – A self-signed certificate, its signature is verified by the public key, which is embedded in the certificate.

By default, these files are stored in the SSL directory in the VMware ACE Management Server program directory.

The self-signed certificate, which is a public certificate, is valid for 10 years from the date and time at which the server is installed. The certificate file is encoded in PEM format.

To browse the file to see its properties

1 Do one of the following:

- In Windows Explorer, navigate to the location of the server.crt file and double-click the file name.
- On a Linux host system, use this command:

```
openssl x509 –in /var/lib/vmware/acesc/ssl/server.crt –text
```

NOTE To replace an expired certificate, deploy the affected ACE-enabled virtual machines in an update package, which includes the new certificate. Do not modify certificates to make them permanent.

When an ACE-enabled virtual machine connects to an ACE Management Server, it downloads the public certificate for that server and any *chain of certificates* required to verify the server's public certificate. A server certificate might have a chain of several

certificates that must be verified step by step until the verification process reaches the root (trusted) certificate in the certificate store. The first time a connection is made to a server by any ACE-enabled virtual machine on a Workstation administrator machine, the certificate is downloaded to the Workstation host system.

The store or collection of certificates that is downloaded when an ACE-enabled virtual machine connects to a server is included in each ACE package that you create with that ACE-enabled virtual machine. It is saved in the ACE Resources directory. When you deploy and run an ACE instance of this ACE-enabled virtual machine, the VMware Player application uses the certificates included in the package to verify connections made to ACE Management Server. It verifies that the certificates that are in the ACE package match those provided by the server. If they do not match exactly, VMware Player displays an error message and does not run the instance.

NOTE If you change the custom SSL certificate for your ACE Management Server, you need to update the Resource directory for all of your existing ACE instances. You can do this by creating and distributing a custom package that contains only Resources.

VMware Player checks the integrity of the certificate store included in the package every time it communicates with the server.

The VMware Player application does not use any certificates stored in the host system, because their integrity cannot be verified.

NOTE ACE Management Server only supports public key certificates that are signed using the SHA1 algorithm. Any other algorithms result in an error when the ACE instance is deployed.

Because the Player does not trust any certificates stored on the host machine on which it is running and instead relies on a complete certification chain that is included in the ACE package, the use of self-signed certificates is adequate for most security needs.

If, however, your enterprise requires the use of a certificate signed by a certificate authority (internal or commercial), you can set up that type of key-certificate pair for the ACE packages to use. A *certificate authority, or CA*, is an entity that issues and signs public-key certificates, typically for a fee. See "Setting Up Custom Certificates," for details.

Setting Up Custom Certificates

To use custom SSL certificates, either your own self-signed certificates or those of a third-party or internal CA (certificate authority), you must provide the various needed certificate, key, and (in the case of CAs) certificate chain files. These files must be PEM encoded. After you create or obtain these files, place them in the correct directory by

uploading them from the Custom SSL Certificates page in the server setup Web application.

Workstation only supports certificate signatures that use the SHA1 algorithm digest.

Perform the following steps to set up your own self-signed certificates, third-party signed certificates or certificates from an internal certificate authority:

1 Ensure that you configured ACE Management Server through the server configuration Web application.

2 Create or provide the needed files:

- For your own self-signed certificate, use `openssl` to create a new self-signed certificate.
- For a third-party CA or internal CA, obtain an SSL certificate signed by that CA, and a certificate-verification chain file.The chain file is a concatenation of every certificate required to verify the new SSL certificate you created or obtained.
- A private key file.

All these files must be PEM-encoded.

Steps for obtaining the certificate chain vary depending on which host operating system you are using and on the source from which the CA certificate is obtained.

3 Rename the files in Step 2 as follows:

- Rename the private key file to `server.key`.
- Rename the certificate file to `server.crt`.
- Rename the certificate chain file to `chain.crt`.

4 Use ACE Management Server configuration Web application to upload the files.

See Step 5 on page 43, under "Configuring ACE Management Server."

5 Stop and restart the Apache service.

See "Stopping and Starting the Apache Service Manually" on page 46.

6 Perform the following steps to update any existing ACE-enabled virtual machines to use a new certificate and key file:

a Open the ACE-enabled virtual machine.

b Create an update package.

The package contains the new certificate file and certificate chain.

Configuring Multiple ACE Management Servers to Use SSL

You might configure multiple ACE 2 Management Servers to use SSL in the following scenarios:

- Multiple servers behind one or more proxy servers:
  - Each server can have its own SSL key and certificate (ACE Management Server and proxy server).
  - The `cert_chain` file must contain the certificate file and verification chain for the SSL certificates that the proxy servers are using. Place this `cert_chain` file in each ACE Management Server.
  - When self-signed certificates are being used, the actual certificate is the verification chain, so the chain file contains each self-signed certificate being used by the proxies.
  - You can also use the same key and certificate for every server and proxy. In this case, it is not necessary to create a `cert_chain` file.
  - Each certificate must have a unique common name.
- Multiple servers using DNS round robin:
  - Each server can have its own SSL key and certificate (ACE Management Server and proxy server).
  - The `cert_chain` file must contain the certificate and verification chain for every certificate being used by the servers. Place this certificate chain file in each ACE Management Server. (Follow instructions above on how to do that.)
  - In the case of self-signed certificates being used, the actual certificate is the verification chain, so the chain file would contain each self-signed certificate being used by each of the servers.
  - It is also possible to use the same key/certificate for every server. In this case, it is not necessary to create a `cert_chain` file. If you use CA-signed certificates, see <cross-reference>.
- Multiple servers without any round robin or behind any proxy servers don't require any special steps. Because no DNS round-robin or proxy server exists, the ACE-enabled virtual machine behaves as if it can talk to only one.

Configuring ACE Management Server

After you install ACE Management Server, you must use the ACE Management Server Setup Web application to configure the server.

You need to provide your ACE Management Server license before you can configure the server features.

Before you start the server setup application, you must complete the tasks described below

Prerequisites for Configuring the Server

If you plan to use Active Directory integration (using LDAP), an external database, or custom SSL certificates, you must complete the following procedures that are applicable to your ACE Management Server option. When these procedures are finished, you can proceed to start the server setup Web application to configure the server.

- "Obtain Your ACE Management Server License Information" on page 34
- "Using Active Directory Integration by using LDAP" on page 34
- "Using an External Database" on page 35
- "Using an External Database with the ACE Management Server Appliance" on page 39
- "Setting Up Custom Certificates" on page 31

Obtain Your ACE Management Server License Information

Obtain your serial number for ACE Management Server before you begin using the server setup Web application to configure the server. If you do not have a serial number available at the initial server configuration, you cannot complete the configuration. As a result, ACE Management Server functionalities are unavailable.

Using Active Directory Integration by using LDAP

This section describes how to use Active Directory integration.

To use Active Directory integration by using LDAP

1 Create a user that ACE Management Server can use to connect to the LDAP server and use for querying.

Make a note of the user principal name (UPN) for that user. For example, create a user called `aceuser` whose UPN is `aceuser@vmware.com`.

2 Create an ACE Administrators group in the domain.

3 Add ACE administrator users to the ACE Administrators group.

4 (Optional) Create a Help Desk group and assign users to it for the Help Desk role.

NOTE You can log in to the Help Desk Web application with your administrative LDAP credentials or password. Creating a Help Desk role allows you to permit certain users to perform Help Desk tasks from within the Help Desk application but does not give them access to other administrative tools.

Using an External Database

This section describes how to use an external database.

To use an external database

1 Install the RDBMS:

- **Windows** – Microsoft SQL Server 2000 or later and Oracle Database 10*g* are supported.
- **Linux** – PostgreSQL 7.4 or later is supported.

The external database does not have to be installed on the same server as ACE 2 Management Server.

ACE Management Server creates the database schema automatically, provided proper access rights are granted.

2 Configure a database.

Ensure that you have a dedicated database and a user account that has full access to this database, including rights to create tables. Ensure that you do not give this database user permissions that it does not need. For example, for reading or writing to other databases that your RDBMS manages.

All tables in the database have a name starting with a `PolicyDb_` prefix and indexes with `PdbIns_` or `PdbLf_` prefixes, so you might provide ACE Management Server with a DSN to a database that it shares with some other application, if the database count is at a premium.

3 (Optional) If you plan to have ACE Management Server connect to the database over the network (TCP socket connection), ensure that the following are in place:

- TCP connectivity is enabled in the database configuration options.
- The TCP connection is not blocked by firewall settings on the database server or the ACE Management Server system.

- You configure each user permission to connect to the database over the network if you are using a PostgreSQL external database. Configure that permission in the `pg_hba.conf` file, which is located in the root folder of your database.

4 (Optional) Verify the server's connectivity to the configured database with the configured user credentials by running a command-line or graphical SQL tool on the ACE Management Server machine.

   Examples of such tools are sqlcmd.exe for SQL Server, sqlplus.exe for Oracle, and psql for Postgres. For database configuration and verification instructions, see the respective database user manual.

5 Create a System DSN entry on the ACE Management Server machine.

   The only required information in DSN configuration is the DSN name, server IP address or host name, and the database name. In other words, you do not need to provide a user name and password in the DSN configuration. Any values entered here are ignored. Provide a user name and password when configuring your ACE Management Server using the Web Setup application.

   Ensure that you create a System DSN and not a user DSN. If you create a User DSN, it is visible only to your user account. ACE Management Server runs under the local system account, so a User DSN is not visible to nor usable by the server.

   - **Windows-based systems** – Using the ODBC Data Sources plug-in (**Control Panel > Administrative Tools > Data Sources (ODBC)**), create a System DSN entry for connecting to this database using the proper driver (see your operating system and database documentation).

     ACE 2 does not support ODBC using an SQL Native Client driver on Windows 64-bit systems.

     If the DSN Setup wizard provides this option, test the connection to verify that it is working with the database user credentials.

     If your ACE Management Server is running on a 64-bit Windows host system, do not use the default Control Panel plug-in to create the DSN. Using that default plug-in will result in your creating a DSN for a 64-bit subsystem, and that DSN will not be visible to ACE Management Server. Instead, navigate to `%WINDIR%\syswow64\odbcad32.exe`, and use that program to create a DSN for a 32-bit subsystem.

- **Linux-based systems** – The `unixODBC` RPM package must be installed on your Linux system for the external database option to be available in the ACE Management Server Setup Web application.

  The `unixODBC` package provides an ODBC API to programs running on Linux systems that is similar to the Windows ODBC API. The package contains the `libodbc` shared library, providing the ODBC Driver Manager API to other programs, a set of configuration utilities, and ODBC drivers for popular databases. On both RHEL4 and SUSE Linux Enterprise Server 9, the ODBC driver for PostgreSQL is included in the `unixODBC` binary distribution package. To use the X11 graphical configuration tool `ODBCConfig` for setting up a DSN on your SUSE Linux Enterprise Server 9 system, the `unixODBC-gui-qt` package must also be installed (this utility is included in the RHEL `unixODBC` package).

  Because `libodbc` is a shared library that implements industry-standard ODBC APIs, ACE Management Server is not sensitive to the particular version of the `unixODBC` package installed on your Linux system, but VMware recommends that you update the package to the latest version released for your specific Linux distribution.

  The DSN configuration for the `unixODBC` package is stored in the `/etc` directory (`/etc/unixODBC` for SUSE Linux Enterprise Server) on your system (`odbc.ini` for DSNs and `odbcinst.ini` for driver and general ODBC system configuration). You can edit these plain-text files manually, or with the `ODBCConfig` graphical (X11) utility. You must be logged in as a root user to access the configuration files or run the ODBC Config utility.

  If you are using the ACE Management Server appliance, see "Using an External Database with the ACE Management Server Appliance" on page 39.

  The `ODBCConfig` utility mimics the Windows ODBC Data Sources Control Panel plug-in. When configuring a DSN for your database connection, ensure that you are using the correct ODBC driver (typically, `/usr/lib/libodbcpsql.so` or, on SUSE Linux Enterprise Server 9, `/user/lib/unixODBC/libodbcpsql.so.2`). You also must configure the server address and the database name in the DSN settings.

  For additional information about using `unixODBC`, see http://www.unixodbc.org/

6 Make a note of the database DSN, user name, and password.

  Enter that information during server setup.

Performance Optimization Tips for External Database Use

For the optimal server performance, ACE Management Server starts multiple parallel threads (on Windows) or processes (on Linux) listening for the incoming connections from the clients. Every client connection typically executes a database transaction, so it needs to open a database connection. Under a high load, all available listening threads or processes might be processing client requests at the same time, so that ACE Management Server requires at least as many database connections available for its use. If the server runs out of database connections, the clients might start receiving connection errors.

For smooth operation of a server with an external database option, ensure that the server has a sufficient amount of database connections available. The maximum number of remote connections allowed to the database is a database configuration option (for information about how to configure it, check your database manual). Configure at least as many connections as potential parallel threads or processes in the Apache HTTP server running the ACE Management Server component, or allow an unlimited number of connections.

To determine the number of parallel threads or processes that an Apache server might start, inspect the Apache configuration file for the prefork or MPM section. The number of allowed clients is the lower bound for the required number of database connections. You can either reduce this number or increase the number of the allowed remote connections in the database.

As a rough guide, here is the location of the Apache configuration file for each platform and the typical default number of connections:

- Windows:

  ```
  C:\Program Files\VMware\VMware ACE Management Server\Apache2\
                conf\httpd.conf
  ```

  250 client connections (WinNT MPM section)

- Linux RHEL 4:

  ```
  /etc/httpd/conf/httpd.conf
  ```

  256 client connections (prefork MPM section)

- SUSE Linux Enterprise Server 9:

  ```
  /etc/apache2/server-tuning.conf
  ```

  150 client connections (prefork MPM section)

- ACE Management Server:

  ```
  /etc/httpd/apache2.conf
  ```

20 client connections (prefork MPM section)

The default installation of the PostgreSQL database on RHEL Linux allows 100 remote connections, which is less than the number of parallel threads started by the Apache server by default on the same platform, so you might want to change this number if you expect a high volume of client requests to your server (if you have more than 100 active clients).

Enabling Database Connection Pooling

Enable database connection pooling in the ODBC Driver Manager (it is disabled by default) to optimize performance for servers on Linux platforms.

On Windows platforms, ODBC connection pooling is enabled by default.

To enable database connection pooling on Linux platforms

1 Start the ODBCConfig utility as a root user.

2 Click the **Advanced** tab.

3 Select the **Connection Pooling** check box.

Enabling this option can give a substantial performance gain under high loads because ACE Management Server can reuse database connections rather than opening new connections for every request.

Using an External Database with the ACE Management Server Appliance

The ACE Management Server appliance does not contain a PostgreSQL database server. You must use an external server to which the server appliance connects over the network. Consider whether an appliance version of a database server would suit your setup.

To set up an ODBC connection to a PostgreSQL external database

1 Log in to the server appliance console as `root`, using the password you created during your first run of the server appliance.

2 Open the `/etc/odbc.ini` file in a text editor.

For example:

```
vaos# vi /etc/odbc.ini
```

This file contains the `postgres_dsn` setting for the OBSC DSN.

3 Uncomment all lines in the `postgres_dsn` file except the first two.

To uncomment lines, delete the pound symbol (#) at the beginning of each line.

4 Replace placeholders <...> with the PostgreSQL database server DNS name or IP address and the database name in this server.

5 Configure the port number as follows:

- Using a non-default port number – Use that port number
- Using the default port number – Keep the default setting

6 Save the file.

These steps ensure that "`postgres_dsn`" appears in the drop-down menu on the **Database** tab in the server setup application.

Using the ACE Management Server Setup Application

Ensure that you all preconfiguration tasks are complete.

To configure the server

1 Start up the configuration application:

- **Windows –** Choose **Start > VMware > VMware ACE Management Server** and click the Configuration link.
- **Linux –** Open a browser, navigate to the address for the host system on which you installed the server, and open the Web page. Click the **Configuration** link.

2 Check the configuration status on the Welcome page:

- If this page says **This server has not been configured**, click **Start**.
- If this page says **This server is configured**, click the tab for the page on which you want to make a configuration change.

3 Set up the license on the Licenses page:

a Enter the serial number for the server.

b (Optional) Enter a user name and company name.

c Click **Next.**

If you are reconfiguring the server, the current licensing information is displayed at the top of the page. The **License Expiration** field shows either **No Expiration** or a date, for permanent and expiring licenses, respectively.

If the system on which you installed ACE Management Server currently has more than one valid server license, just one license is displayed on that page.

4 (Optional) Change license information:

a Click **Change**.

b (Optional) Enter the new user name or company name.

c Enter the serial number.

If you are not changing the serial number at this reconfiguration, enter the existing number.

d Click **Apply** and **Restart** or **Later**.

If you click **Later**, you need to restart the server manually.

5 On the Database page, select a database option:

- **Embedded Database** – Uses the default embedded SQLite database engine. Then click **Next**.
- **External Database (ODBC-compatible)** – Uses an external database, either Microsoft SQL Server or Oracle Database 10*g* (Windows) or PostgreSQL (Linux). Provide the database DSN, user name, and password.

  After you enter the database connection credentials, the setup application checks for an existing database. If the database is present, the setup application offers an option to re-initialize it (erase all data, restoring the database to its default state; the default setting for the option is No). You can also use the reinitialization option at a later time (after setup is complete, by revisiting this page) to reset the database.

  If the database setup is unsuccessful, the server setup fails and the server cannot start.

  If you are upgrading the server from the previous release, the database schema is upgraded automatically and you do not lose your previous data. The upgrade is done on the first start of the upgraded server, even if you do not rerun the setup application. For information about upgrading from a previous ACE 2 release, see the release notes.

Continue with the server configuration in one of the following ways:

- If you are configuring the server for the first time, click **Next**.
- If you are reconfiguring the server, click **Apply** and then click **Restart** or **Later**. If you click **Later**, you must restart the server manually.

6 (Optional) Integrate ACE Management server to an existing LDAP directory.

a On the Access Control page, select **Domain Account (LDAP)**.

b Specify credentials that the ACE Management Server uses to connect to and query the domain controller:

- **Host Name** – Enter the host name of the LDAP server, using the name you created during the Active Directory integration procedure.
- **Query User UPN** – Enter the UPN for the LDAP server. Together with the Query User Password, the Management Server uses this parameter to connect to the LDAP server.
- **Query User Password** – Enter the password for the query user.
- **Default Domain** – Enter the default domain on which you authenticate users.

The query user can be any user who has read access to the locations where user and group objects reside in the LDAP server.

c Click **Next** or **Apply**.

d Select the ACE Administrators group.

The administrator uses the specified group to authenticate and authorize users. You set up this group when you prepared for Active Directory integration before you started the server configuration.

e To set up a separate role for the Help Desk application, enable **Helpdesk LDAP Group** and select a group to log in to the application.

If this option is not enabled, anyone who logs in to the Help Desk application must be a member of the ACE Administrators group.

7 (Optional) Specify the password for ACE Management Server administrators.

Administrators must enter this password before they can modify the server's configuration.

This step is only necessary if you do not plan to use an Active Directory service. To enable a role for using the Help Desk Web application, select **Enable Helpdesk Role** and specify a password that users must enter when they start up the Help Desk application.

If you are reconfiguring the server, any passwords you entered previously are shown as a 12-character display rather than as the actual number of password characters.

Deleting the ACE Management Server Configuration File and Setting a New Administrator Password

If you used complex settings in your configuration file, you might want to save a copy of the file so that you can look at those settings while you are reconfiguring the server.

To delete the ACE Management Server configuration file and set a new administrator password

1 Navigate to the location of the ACE Management Server configuration file:

- **Windows** – `C:\Program Files\VMware\VMware ACE Management Server\conf\acesc.conf`
- **Linux** – `/var/lib/vmware/acesc/conf/acesc.conf`

2 Delete the configuration file.

3 Navigate to the server setup Web application and configure the server again, specifying a password on the Access Control page.

4 Continue with the server configuration in one of the following ways:

- If this is the initial configuration of the server, click **Next**.
- If you are reconfiguring the server, click **Apply** and then click **Restart** or **Later**. If you click **Later**, you will need to the server manually.

5 (Optional) To use custom SSL certifications, upload the PEM-encoded files to the correct directory.

a Click the appropriate **Browse** button to navigate to and upload the key and certificate files you created.

b (Optional) If you are using CAs, upload the chain file.

c Click **Upload certificates**.

d Verify that the summary page shows that the correct files were uploaded.

If you upload an invalid certificate file, the server setup application fails when you click **Apply** and then **Restart** and you cannot restart the Apache service. To fix this problem, restore the backup certificate file for the corresponding certificate. The backup certificate files are in the following format:

`<certificate_filename>.<date>-<time>`

where `<certificate_filename>` is one of:

`server.crt` for the server public certificate

`server.key` for the server private key

`chain.crt` for the certificate chain

`<date>` is in the format YYYYMMDD (year, month, day).

`<time>` is in the format HHMMSS (hours, minutes, seconds).

The backup files are in the ACE Management Server directory, with the filename appended with the date and time; for example, `server.crt.20070216–095344`.

Save the file in the correct location as `ssl/<filename>.crt` and restart the Apache server manually to complete the restoration process and to bring up the VMware ACE Management Server Setup Web application again and continue the configuration.

e Click **Close** to close the summary page.

f Continue with the server configuration in one of the following ways:

If this is the initial configuration of the server, click **Next**.

If you are reconfiguring the server, click **Apply** and then click **Restart** or **Later**. If you click **Later**, you must restart the server manually.

6 (Optional) Set logging options:

a Set the log-type categories.

Each category covers several server RPC interfaces and contains several distinct event types. The categories are:

ACE Administration – Logs events for ACE instance creation, update, and destruction.

Package Administration – Logs events for package creation and update.

Policy Administration – Logs events for policy-set update and publish, instance customization, and user access control changes by an ACE administrator.

Instance Administration – Logs instance life-cycle events: creation, copying, revocation, reenablement, and deletion, instance password change by a user, instance password change by an administrator, changes of per-instance expiration, changes of instance guest or host OS information, and setting instance custom fields. The debug level can be used to log the most ubiquitous traffic such as policy update requests from active instances. Failed instance verifications are only logged at the debug level.

Authentication – Logs events for every authentication request. Administration or help desk authentication attempts (at the normal level), instance authentication (at the informational level), and remote LDAP password change. You might want to set logging for this category to as minimal a level as is practical for you; otherwise, this category can generate a large volume of entries.

b Set the detail level individually for each of the logs:

None – No log entry is made for this event.

Critical – The log provides entries for the critical category of events, which are those having broad and critical effects. for example, an event that removes all packages, instances, and policies associated with an ACE-enabled virtual machine.

Normal – The amount of information given in the entry is sufficient to answer most queries.

Informative – The log provides entries for nondestructive events that have limited effect.

Debug – The log provides entries for every client access of the server. It provides more records of certain event types, creating potentially orders of magnitude more logging entries than other log levels. It logs all informational transactions, such as instance status and so on. Use this setting only when debugging running servers in the field.

c Use the **Event Log Purging** feature to specify whether to keep log entries indefinitely, keep log entries for at least a minimum specified number of days, or keep at least a minimum specified number of log entries after each purge.

The oldest entries are purged first. The purge maintenance process runs approximately every six hours.

d Continue with the server configuration in one of the following ways:

If you are configuring the server for the first time, click **Next**.

If you are reconfiguring the server, click **Apply** and then click **Restart** or **Later**. If you click **Later**, you must restart the server manually.

A message indicating that serve setup is complete appears

7 Click **Restart**.

If you click **Later**, you must manually restart the server for the configuration changes to take effect. The new configuration is written. You must restart the system for ACE Management Server to use the configuration.

8 On the Login page, type your admin password and click **Login**.

9 Close the window.

Related Topics

- "Stopping and Starting the Apache Service Manually" on page 46
- "Using Active Directory Integration by using LDAP" on page 34
- "Using the VMware Help Desk Web Application" on page 49
- "Setting Up Custom Certificates" on page 31

Using Event Logs

The server collects log entries for events that change the database. You can set the logging levels and set an option for purging log entries.

Related Topics

"Configuring ACE Management Server" on page 34

Stopping and Starting the Apache Service Manually

This section describes how to restart the Apache service on each of the supported server types.

To manually restart the Apache service on a Windows host server:

1 Click the Apache icon in the taskbar.

2 Click **Stop** and then click **Start**.

Ensure that you click **Stop** and **Start**, not **Restart**.

To manually restart the Apache service on a Red Hat Linux 4 host server

1 Log in to your host console.

2 As `root`, type the following command:

```
/etc/init.d/httpd stop
/etc/init.d/httpd start
```

To manually restart the Apache service on a SUSE Linux Enterprise Server 9 SP3 host server

1 Log in to your host console.

2 As `root`, type the following command:

```
/etc/init.d/apache2 stop
/etc/init.d/apache2 start
```

To manually restart the Apache service on the ACE Management Server appliance

1 Log in to your host console.

2 As `root`, issue the following command:

```
/etc/init.d/apache2 stop
/etc/init.d/apache2 start
```

Logging In to ACE Management Server

Communications between Workstation and ACE Management Server take place over a secure SSL connection.

When you attempt to access ACE Management Server for the first time in a Workstation session, a login dialog box appears. You need to supply the appropriate login information:

- If the server is not integrated with Active Directory service, enter the administrator password that you set when you configured the server.
- If the server is integrated with Active Directory service, enter your administrative credentials (user name, password, and domain) in one of the formats shown in Table 3-2.

Table 3-2. Login Options for ACE Management Servers with Active Directory Service

Option	Description
long name + password + domain name	The long name is the “First_name Last_name” format, for example, “ACE User”.
long name + password	The long name is the “First_name Last_name” format, for example, “ACE User”. Leave the domain field blank.
short name + password + domain	The short name is the sAMAccountName, for example, “ace” as the shorter form of long name “Ace User”.
short name + password	The short name is the sAMAccountName, for example, “ace” as the shorter form of long name “Ace User”. Leave the domain field blank.
email address + password	This option can only be used for a domain that is accessed through a direct connection. Leave the domain field blank.

Table 3-2. Login Options for ACE Management Servers with Active Directory Service

Option	Description
NETBIOS DOMAIN NAME\username + password	The NetBIOS name is a short name for domains that is registered in the NetBIOS Name Service (WINS). Leave the domain field blank.
username + password + NETBIOS DOMAIN NAME	The NetBIOS name is a short name for domains that is registered in the NetBIOS Name Service (WINS).

Using ACE Management Server

After ACE Management Server is installed and configured, you can use it to accomplish these tasks:

- View the instances on the server in the Workstation user interface.
- Revoke and re-enable an instance.
- Push out a dynamic policy update.
- Fix various problems with the ACE instances as reported by instance users, through the Instance View in the Workstation interface or through the Help Desk Web application.

See Chapter 4, "Instance Management," on page 55 and "Using the VMware Help Desk Web Application" on page 49.

Connection Problems Between a Linux ACE Instance and ACE Management Server

If your ACE instance on a Linux host computer cannot contact the server, check to see whether a firewall or proxy setting is blocking or rerouting https traffic on port 443. By default, https traffic from the VMware Player to ACE Management Server is routed on port 443. Disable the firewall or turn off the proxy setting to allow Player-to-server traffic on that port.

Change the Port Assignment for ACE Management Server

ACE Management Server is a module running on the Apache 2.0 platform. To change the port that the server listens on, you must manually edit the Apache configuration file.

To change the port assignment for ACE Management Server

1 Using a text editor, open the ACE Management Server component http configuration file.

- **Windows** – `C:\Program Files\VMware\VMware ACE Management Server\Apache2\conf\httpd.conf`
- Red Hat Enterprise Linux 4 host server – `/etc/httpd/conf.d/acesc.conf`
- SUSE Linux Enterprise Server 9 SP3 host server – `/etc/apache2/conf.d/acesc.conf`

  This path is different if VMware ACE Management Server is installed in a different location. Use the path you established for your server.

2 Locate the line entry in the file that reads `Listen 443` and change the port number.

  The server uses port 8000 for configuration, and the ACE Management Server appliance uses port 8080, so you cannot choose those ports.

3 Locate the Virtual Server configuration for port 443.

```
<VirtualHost –default_:443>
```

  It starts with the preceding line and ends with the following line:

```
</VirtualHost>
```

4 Change the port number in the section header to the desired port number.

  For example, to change to port 8443, change `443` to `8443`.

5 Save the file.

6 Stop and start the Apache service.

ACE Management Server is now listening on the specified port.

When you create an ACE-enabled virtual machine, you can specify which port is to be used to talk to ACE Management Server.

Related Topics

- "Stopping and Starting the Apache Service Manually" on page 46

Using the VMware Help Desk Web Application

The VMware Help Desk Web application allows help desk assistants or administrators to view ACE instances that are managed by a particular VMware ACE Management Server and to provide some fixes requested by users of those instances.

Help desk assistants can access the ACE instance through the VMware Help Desk Web application and can fix just a limited set of ACE instance problems, such as reactivating an instance, changing the instance's expiration date, or resetting the user password if the user has lost or forgotten it.

To set up a password for help desk assistants: Open the ACE Management Server Setup Web application (see "Using the ACE Management Server Setup Application" on page 57 for information for details) and choose **Enable Help Desk Role** on the Access Control tab. Type in a help desk password and confirm the password.

To access the Help Desk application on Windows

1 Choose **Start > All Programs > VMware > VMware ACE Management Server**.

2 Click the Help Desk link.

To access the Help Desk application on Linux

1 Open a browser and point it to `https://<hostname>:8000`.

2 Click the **Help Desk** link.

The VMware Help Desk opens the Instances page, which contains a summary table of all the instances that server manages.

Managing Instances

Use the VMware Help Desk's Instances page to manage a server's instances. To navigate through the Instances page, click the previous and next arrows at the right of the status bar at the bottom of the Instances table. The indicator at the left edge of the status bar displays which instances of the total number of instances that this server manages are shown on this page. For example, "11 - 20 / 150" indicates that instances 11 through 20 of 150 instances appear on the current page.

Search for Instances

You can use the advanced search function in the VMware Help Desk to query the ACE 2 Management Server database to find one or more particular ACE instances.

To search for an ACE instance

1 Click **Search** in the upper left of the Instances page.

Specify the criteria to be included when the database is queried by entering data in the fields to be queried.

Field	Description
Activated by	Refers to the activation method, such as password or activation key. If no such activation method exists, N/A appears in the column.
Activated	
Deactivated	
Valid	
ACE-Enabled Virtual Machine Name	
Package Name	
Host Name	
Host IP Address	
Guest Name	The Guest Name, which is the computer name resolved on the user's machine during instance customization (a feature for Windows systems only), always appears in the help desk view as 15 characters or fewer. The NetBIOS name is reported here, and it is a maximum of 15 characters long. Even if the actual computer name contains more characters, the name always appears as the NetBIOS name.
Guest IP Address	
Guest MAC Address	

Any custom columns that you specified appear directly below the Guest MAC Address criterion.

If you select the **Exact match only** option for a search category, only instances with values that are exact matches of the value specified in that category field are listed in the search results. Exact-match values are case-sensitive.

Specify dates in the format MM/DD/YYYY.

Search criteria are joined with AND, not OR, operations.

You can save a search by entering a name in the Save as field in the Advanced Search dialog box. Saved searches are specific to each server. If you go to the instance view of another server, that server has a unique set of saved searches. You

can edit or delete your saved searches by selecting the name of a saved search in the **Saved Searches** drop-down menu and clicking **Options**.

Click **Reset** in the Search dialog box if you want to clear entries in the search fields.

2 Click **Search**.

The Search dialog box closes and the search results appear.

3 Click **Back to all instances** in the upper left of the window if you want to refresh the display with the total list of instances.

4 If the results list cannot all be displayed on one page of the Instances table, you can click the Next arrow at the bottom right of the table to see the next page of results.

Reactivate or Deactivate an Instance

You can immediately deny or allow access to an instance by deactivating or reactivating it.

To reactivate or deactivate an instance

Select the instance by clicking the instance row once, and then click the appropriate icon, **Deactivate** or **Reactivate**, in the upper-left corner of the Instances page.

The change is made as soon as you click the icon.

To reset the expiration dates for an expired instance

1 Select the instance row and click **Reactivate**.

2 Reset the expiration dates in the dialog box and click **OK**.

Sort Instances by Column Heading

You can reorder the instances in the table alphabetically or numerically, depending on the selected column's contents, in ascending or descending order.

To reorder a column alphabetically or numerically

Click to the right of the column heading of the column to sort.

Click again to re-sort in the opposite (ascending or descending) order.

To change column widths

Click on a column divider and drag the column edge to a new width.

To access the instance details page

Double-click the instance row.

View Details for the Instance

General details for the instance appear at the top of the Instance Details page. The rest of the page provides details about any instance customization results, the guest MAC address, and the various policy settings. Removable devices shows the settings for the removable devices policy, including details about which devices are allowed and blocked. For more information about the display for network access policy settings, see "View Network Access Details" on page 54.

Reactivate and Deactivate an Instance

You can immediately deny or allow access to an instance by deactivating or reactivating it.

To reactivate or deactivate an instance, click the appropriate icon, **Deactivate** or **Reactivate** in the upper-left corner of the Instance Details page. The change is made as soon as you click the icon.

Reset an Instance Expiration Date

You can reset an expiration date by selecting or deselecting **Use the date range specified for the ACE-enabled virtual machine**, entering **Valid From** and **Valid Until** dates, and selecting or deselecting **Never expire**. Click **Save** in the upper-left corner of the page to apply the new expiration date.

Change Copy Protection ID

You can change copy protection ID to allow a user to run a moved or copied instance. Select the alphanumeric string in the **Copy Protection ID** field and replace it with the new copy protection ID.

The **Copy Protection ID** field is always active, so you can change the ID at any time.

CAUTION If you enter a change in the **Copy Protection ID** field for an active instance, a warning appears to let you know that if you change the ID, the original instance no longer runs.

Click the **Save** button in the upper-left corner of the page to apply the new ID.

Reset the Password

You can reset passwords for instances with user-specified passwords. Click **Reset Password** and specify a new password. The new password must have at least one character. Send the new password to the user in an e-mail message.

The change is made as soon as you click **OK** in the Password dialog box.

View Network Access Details

Click the links under **Zone**, **Host Access,** or **Guest Access** to view the Zones or Rules Detail page for this zone or this type of network access.

Instance Management 4

The Instance View provides you with a central management point for all instances that a particular ACE Management Server manages. A summary table provides instance status (activated, deactivated, or blocked by policy violation) and expiration dates for the instances, as well as details such as who activated the instance, the ACE-enabled virtual machine, package name, guest name and IP address, and host name for this instance.

You can select an instance in the table and deactivate or reactivate the instance. A details view for each instance shows the instance's general statistics and policy settings.

This chapter discusses the following topics:

- "Viewing All Instances that a Server Manages" on page 56
- "Searching for Instances" on page 56
- "Managing Columns in the Instance View Table" on page 58
- "To change the Instance table sort order" on page 58
- "Type the new name in the Name field of the Custom Column Name dialog box and click OK." on page 59
- "To reset expiration dates for an expired instance" on page 59
- "To open a Details View" on page 60
- "To open an Instance View with the Connect to ACE Management Server command" on page 62

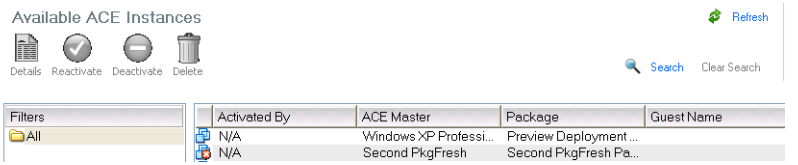
Beta

Viewing All Instances that a Server Manages

To view all instances that a server manages

1 Click the server name in the sidebar.

Figure XX shows an example of an Instance view.



An instance has one of the following status types:

- **Active** – The instance is active and available for immediate use.
- **Blocked by policies** – The instance is still active but is blocked (cannot be run) because of a violation of a policy such as expiration date or copy protection. For details on the reason for a blockage, view the server log for that instance.
- **Deactivated** – This instance was purposely deactivated. You must reactivate it to make it usable again.

The **Valid From** and **Valid Until** column indicate the period that the instance is valid. The instance expires after the **Valid Until** date. If no expiration date is set for the instance, those columns are empty.

Searching for Instances

Use the advanced search function in the Instance View to query the ACE Management Server database to find one or more particular ACE instances.

To search for an ACE instance

1 Click **Search** in the upper-right corner of the Available ACE Instances page of the Instance View.

2 Specify the criteria to be included when the database is queried.

In the date fields, you can enter a start date and leave the end date empty.

Option	Description
Activated by	
Activated	

Beta

Option	Description
Deactivated	
Valid	
ACE-Enabled Virtual Machine Name	
Package Name	
Host Name	
Host IP Address	
Guest Name	The Guest Name, which is the computer name resolved on the user's machine during instance customization (a feature for Windows systems only), is always shown in the Instance View as 15 characters or less. The NetBIOS name is reported here, and it is a maximum of 15 characters in length. Even if the actual computer name contains more characters, the name is always shown as the NetBIOS name.
Guest IP Address	
Guest MAC Address	

3 To search on custom columns, select **Show custom values** and specify the search values for those columns.

If you select the **Exact match only** option for a search category, only instances with values that are exact matches of the value specified in that category field are listed in the search results. Exact-match values are case sensitive.

Specify dates in the format MM/DD/YYYY.

Search criteria are joined with AND, not OR, operations.

4 To save a search, enter a name in the **Save as** field in the Advanced Search dialog box.

Saved searches are specific to each server. If you go to the instance view of another server, that server has a unique set of saved searches.

5 To edit or delete saved searches, select the name of a saved search in the **Saved Searches** drop-down menu and click **Options**.

6 Click **Search**.

Beta

The search results appear. An indicator in the lower-right corner of the page shows the number of results in the view out of the total number of results. For example, **Showing 24 out of 55**.

The query is remembered for the length of the Workstation session.

To clear a query

1 Click **Search** on the Instance View page.

2 Click **Reset** in the Advanced Search dialog box.

3 Click **Search**.

Managing Columns in the Instance View Table

You can show, hide, and move, and resize the width of columns that appear in the Instance View table.

NOTE The column setup, the visible columns and their positions, is saved for each server view you work with. If you rearrange the view for one server, the views of other servers that you open are not affected by that rearrangement.

To show columns

To show or hide a column, right-click the column heading row and select or deselect the column to show or hide. If you show a column that was previously hidden, the column is added to the right side of the table.

To move a column

To move a column, click the column header, drag the column to a new location, and release the mouse button.

To resize a column

To resize column width, click on the right side of a column divider and drag the column edge to a new width.

To change the Instance table sort order

Right-click the column heading and choose **Sort**.

Managing Custom Columns

You can create up to nine custom columns in the Instance View table so that you can view additional categories of information about the instances that the server manages.

Beta

In the Instance View table, you can add, delete, and rename custom columns.

To specify a value that will appear in a custom column, go to the Details view for the instance. See "Creating Custom Columns" on page 61.

To add a custom column

1 Right-click anywhere in the column heading row and choose **Add Custom Column**.

2 Type a name for the new column in the **Name** text box and click **OK**.

NOTE After you add nine custom columns, the **Add Custom** command in the right-click menu is dimmed and you cannot select it. You must delete one of the nine existing custom columns before you can add another one.

To delete a custom column

- Right-click on the column header for the custom column and choose **Delete Columns** from the context menu.

To edit a custom-column name

1 Right-click on the column header for the custom column and choose **Edit Title**.

2 Type the new name in the **Name** field of the Custom Column Name dialog box and click **OK**.

To deactivate an active instance

1 Click the instance in the right pane of the view.

2 Click the **Deactivate** icon at the top left of the view.

Verify that the icon is dimmed.

To reactivate a deactivated instance

1 Click the instance in the right pane of the view.

2 Click the **Reactivate** icon at the top left of the view.

3 Verify that the icon is no longer dimmed.

To reset expiration dates for an expired instance

1 In the Instance View, select the instance row.

Ctrl+click or Shift+click to select multiple instances and then reactivate or deactivate them all at once.

Beta

2 Click **Reactivate**.

3 Enter a new expiration date.

4 Click **OK**.

To open a Details View

Double-click the instance row in the right pane of the view.

Viewing General Statistics

The **General Details** view shows statistics for this instance, including the following:

- Instance number
- Activated by
- Activation status
- ACE-enabled virtual machine name
- Package name
- Activation and deactivation dates
- Expiration date range
- Guest Name
- IP address
- MAC address
- Host name
- IP address

Beta

To activate or deactivate the instance

1 To activate or deactivate the instance, click **Reactivate** or **Deactivate**.

2 Click **OK**.

To reset the instance expiration date

1 To reset the expiration date for an instance, select or deselect **Use the date range specified for the ACE-enabled virtual machine**.

2 Check **No expiration** if you do not want the instance to expire.

3 Click **OK**.

Resetting the Password and Copy Protection ID on the Policies Tab

The **Policies** tab on the ACE Instance Details dialog box shows current policy information for an instance, including the following:

- Date and time that an instance last retrieved the policies from the server
- Current policy values, including the network access table and a list of removable devices
- Copy protection ID

To reset the password for an ACE instance

1 Click **Reset Password**.

2 Type the password in the first text box and retype it in the second text box to confirm it.

3 Click **OK**.

To change the copy protection ID for an ACE instance

1 Select the alphanumeric string in the **Copy Protection ID** text box.

2 Type the new ID over the old ID.

3 Click **OK**.

Generally, the user provides the new alphanumeric string to you with a request to allow a moved or copied instance to run.

The Copy Protection ID field is always active, so you can change the ID at any time.

If you enter a change in the **Copy Protection ID** text box for an active instance, a message tells you that if you change the ID, the original instance will no longer run.

Creating Custom Columns

The **Custom** tab on the ACE Instance Details dialog box shows values for any custom columns that you create.

To specify values for custom columns

1 In the Instance View table, click the row for the instance that has custom columns for which you need to set values.

2 Click the **Details** icon.

Beta

3 Click the **Custom** tab.

4 Type a string value for each custom column in the appropriate text box.

Entries have no character or format restrictions. You can even leave the fields empty.

5 Click **OK**.

To connect to ACE Management Server

1 Choose **File** > **Connect to ACE Management Server**.

2 Enter the server address and port number in the dialog box.

3 Click **OK**.

In addition to using the Connect to ACE Management Server command to open a server connection, you can open the connection by doing one of the following:

- Creating a new master and assigning it to the server
- Opening an existing master that is already assigned to the server
- Opening an existing virtual machine, cloning it to create a new master, and then assigning the master to the server

To open an Instance View with the Connect to ACE Management Server command

Click a server name in the list of Recent ACE Management Servers in the sidebar of the Workstation interface.

Beta

Database Schema and Audit Event Log Data

A

Tables in the VMware ACE Management Server database represent the major configuration objects of ACE Management Server: Ace, Package, Instance, Access Policy, Runtime Policy, and User Data (which contains image customization settings and other per-user data). Administrator and user actions are audit logged in the Event table in the database, while possible event types are listed in the EventType table. This Appendix explains the format of the data stored in the database, and the best ways to access this data.

For a big installation, you might choose to use a third-party database management or reporting tool with the VMware ACE Server database. You might want to create custom reports of the system state using a reporting tool such as Crystal Reports. You can also use a reporting tool to inspect the audit trail of the administrator or user actions stored in the Event table. For example, you might find active instances with outdated ACE policy sets, or excessive failed authentication attempts.

Database Schema

The RDBMS access control mechanism protects the data stored in the database. Do not allow the database user account used by your reporting tool to have a higher than necessary level of access to the data. Otherwise you might compromise the security of your VMware ACE system.

For example, reporting tools typically do not need write access to the database. Instead, you can create a separate read-only account for the reporting tool. You might also want to disallow read access to database fields that contain sensitive information, such as user passwords, instance customization data (which might have the domain administrator logon), or instance disk encryption keys. The embedded SQLite database

does not support authentication, so access can be protected only by "all or nothing" file-based security.

The following is the database schema script.

```
/* Name - value pairs of service information, e.g. DB schema version number */
CREATE TABLE PolicyDb_MetaInfo (
  name VARCHAR(128),                        /* Name of the name-value pair */
  value VARCHAR(1024),                      /* Value of the name-value pair */
  PRIMARY KEY(name));

/* This table holds data for guest and host policy sets, split in 2K chunks */
/* Select all fields for the key in the order of index and append strings together */
/* to reconstruct the policy set */
CREATE TABLE PolicyDb_LongField (
  longFieldKey VARCHAR(128),                /* Unique ID of the long field series */
  longFieldIndex INTEGER,                   /* Index in the series */
  longFieldValue VARCHAR(2000),           /* Up to 2000 chars of field value chunk */
  sessionExpires VARCHAR(21),           /* Optional field for storing session blob */
  PRIMARY KEY (longFieldKey, longFieldIndex));

/* ACE Master data */
CREATE TABLE PolicyDb_Ace (
  aceUID VARCHAR(128),                      /* Unique ID (primary key) */
  aceName VARCHAR(128),                     /* Name of this ace */
  activePolicySetVersion INTEGER NOT NULL,  /* Soft foreign key to active RT policy*/
  aceTsCreated VARCHAR(21) DEFAULT 0 NOT NULL,   /* Creation timestamp */
  aceTsLastModified VARCHAR(21) DEFAULT 0 NOT NULL,  /* Last modified timestamp */
  deleted VARCHAR(7) DEFAULT 'FALSE',       /* Is this entry deleted (tombstone) */
  PRIMARY KEY(aceUID));

/* Package data */
CREATE TABLE PolicyDb_Package (
  packageUID VARCHAR(128),                  /* Unique ID (primary key) */
  aceUID VARCHAR(128) NOT NULL,             /* The ACE it belongs to. */
  pkgName VARCHAR(128),                     /* UI visible name. */
  pkgUseValidDates VARCHAR(7)
     DEFAULT 'FALSE' NOT NULL,              /* Use validity dates or always valid */
  pkgValidDateStart VARCHAR(21) NOT NULL,   /* The package is valid from this date.*/
  pkgValidDateEnd VARCHAR(21) NOT NULL,     /* The package is valid till this date.*/
  pkgDisabled  VARCHAR(7) DEFAULT 'FALSE' NOT NULL,  /* Is the package disabled */
  pkgProtectionKey VARCHAR(1024),         /* The key used for package distribution */
  pkgPreview VARCHAR(7) DEFAULT 'FALSE' NOT NULL, /* Is preview package */
  pkgTsCreated VARCHAR(21) DEFAULT 0 NOT NULL,   /* Creation timestamp */
  pkgTsLastModified VARCHAR(21) DEFAULT 0 NOT NULL, /* Last modified timestamp */
  deleted VARCHAR(7) DEFAULT 'FALSE',       /* Is this entry deleted (tombstone) */
  PRIMARY KEY(packageUID),
  FOREIGN KEY(aceUID) REFERENCES PolicyDb_Ace(aceUID));

/* Access Control object data (single item of the list, associated with ACE Master)*/
```

```
CREATE TABLE PolicyDb_Access (
  accessPK VARCHAR(128),                    /* Unique ID (primary key) */
  aceUID VARCHAR(128),                   /* Ace for which this access policy is (FK)*/
  identityData VARCHAR(128),                /* Internal representation, SID in AD */
                                            /* case, token value goes here. */
  accVersion INTEGER NOT NULL,              /* Access object version number */
  identityType INTEGER NOT NULL,            /* AD User, Group, or Token Value */
  identityName VARCHAR(128),              /* UI visible user/group name in AD case */
  accUseInstanceLimit VARCHAR(7)
     DEFAULT 'FALSE' NOT NULL,          /* Limit number of instances for this ID?  */
  accInstanceLimit INTEGER NOT NULL,        /* Max no. of ACE instances allowed */
  accTsCreated VARCHAR(21) DEFAULT 0 NOT NULL,   /* Creation timestamp */
  accTsLastModified VARCHAR(21) DEFAULT 0 NOT NULL,  /* Last modified timestamp */
  deleted VARCHAR(7) DEFAULT 'FALSE',       /* Is this entry deleted (tombstone) */
  PRIMARY KEY(accessPK),
  FOREIGN KEY(aceUID) REFERENCES PolicyDb_Ace(aceUID));

/* ACE Instance object data */
CREATE TABLE PolicyDb_Instance (
  instanceUID VARCHAR(128),                 /* VM instance ID (primary key) */
  packageUID VARCHAR(128) NOT NULL,         /* The package it belongs to. */
  aceUID VARCHAR(128) DEFAULT '' NOT NULL,  /* The ACE Master it belongs to */
  creatorIdName VARCHAR(128) NOT NULL,  /* Display name of the activator user      */
  creatorIdData VARCHAR(256),          /* Fully qualified name of the activator   */
  creatorAuthType INTEGER NOT NULL,     /* The type of access check at activation  */
  activationDate VARCHAR(21) NOT NULL,  /* The date and time for the activation.   */
  lastPolicyCheck VARCHAR(21) NOT NULL, /* Last time when the player called server */
  revocationDate VARCHAR(21) NOT NULL,  /* When the instance was revoked */
  replacementDate VARCHAR(21) NOT NULL, /* When replaced because of Copy Protect.  */
                                        /* policy      */
  inheritsExpiration
     VARCHAR(7) DEFAULT 'FALSE' NOT NULL,   /* Use expiration info from Ace Policy
                Set */
  insUseValidDates
     VARCHAR(7) DEFAULT 'FALSE' NOT NULL,   /* Use validity dates or always valid */
  insValidDateStart VARCHAR(21) NOT NULL,   /* The instance is valid from this date*/
  insValidDateEnd VARCHAR(21) NOT NULL,     /* The instance is valid till this date*/
  insPassword VARCHAR(128),                 /* The login password for non-AD */
                                            /* authentication for this instance */
  hostName VARCHAR(128),                 /* The name of the host PC the VM runs on */
  hostIp VARCHAR(128),                  /* The IP addr of the host the VM runs on  */
  insProtectionKey VARCHAR(1024),           /* Instance VM disk encryption key */
  copyProtectionId VARCHAR(1024),           /* Stores location of the copy */
  insPreview VARCHAR(7) DEFAULT 'FALSE' NOT NULL, /* Is preview instance */
  guestIpAddress VARCHAR(128) DEFAULT '',   /* Reported VM IP address */
  guestMacAddress VARCHAR(128) DEFAULT '',  /* Assigned VM MAC address */
  guestMachineName VARCHAR(128) DEFAULT '', /* The guest (VM) OS host name */
  guestConfigStatus INTEGER DEFAULT 0,      /* The completion status of guest */
                                            /* auto-configuration */
  guestConfigMsg VARCHAR(512),              /* Message for the guest auto-config */
```

```
  insTsCreated VARCHAR(21) DEFAULT 0 NOT NULL,   /* Creation timestamp */
  insTsLastModified VARCHAR(21) DEFAULT 0 NOT NULL,  /* Last modified timestamp */
  deleted VARCHAR(7) DEFAULT 'FALSE',       /* Is this entry deleted (tombstone) */
  insCustom1 VARCHAR(255),                  /* User-defined field */
  insCustom2 VARCHAR(255),                  /* User-defined field */
  insCustom3 VARCHAR(255),                  /* User-defined field */
  insCustom4 VARCHAR(255),                  /* User-defined field */
  insCustom5 VARCHAR(255),                  /* User-defined field */
  insCustom6 VARCHAR(255),                  /* User-defined field */
  insCustom7 VARCHAR(255),                  /* User-defined field */
  insCustom8 VARCHAR(255),                  /* User-defined field */
  insCustom9 VARCHAR(255),                  /* User-defined field */
  PRIMARY KEY(instanceUID),
  FOREIGN KEY(packageUID) REFERENCES PolicyDb_Package(packageUID),
  FOREIGN KEY(aceUID) REFERENCES PolicyDb_Ace(aceUID));

/* MAC Address Pool (reserved for future use) */
CREATE TABLE PolicyDb_MacPool (
  macPoolUID VARCHAR(128),                  /* primary key */
  aceUID VARCHAR(128) NOT NULL,             /* ACE for which this MacPool is used */
  macPoolName VARCHAR(128),                 /* User visible name */
  description VARCHAR(128),                 /* name and description of the MAC pool*/
  rangeStart VARCHAR(21) NOT NULL,          /* Start address of the MAC pool */
  rangeEnd VARCHAR(21) NOT NULL,            /* End address of the MAC pool */
  lastAssigned VARCHAR(21) NOT NULL,        /* Last assigned address */
  mplTsCreated VARCHAR(21) DEFAULT 0 NOT NULL,   /* Creation timestamp */
  mplTsLastModified VARCHAR(21) DEFAULT 0 NOT NULL, /* Last modified timestamp */
  deleted VARCHAR(7) DEFAULT 'FALSE',       /* Is this entry deleted (tombstone) */
  PRIMARY KEY(macPoolUID),
  FOREIGN KEY(aceUID) REFERENCES PolicyDb_Ace(aceUID));
/* Instance customization data */
CREATE TABLE PolicyDb_UserData (
  userDataPK VARCHAR(516),                  /* Primary key */
  aceUID VARCHAR(128),                   /* ACE for which this UserData is defined */
  packageUID VARCHAR(128),              /* Package for which this UserData is used */
  activator VARCHAR(128),                   /* The user */
  udataName VARCHAR(128),                   /* User data entry name */
  udataType INTEGER NOT NULL,               /* Attribute of the date */
  udataValue VARCHAR(2048),                 /* User data entry value */
  udtTsCreated VARCHAR(21) DEFAULT 0 NOT NULL,   /* Creation timestamp */
  udtTsLastModified VARCHAR(21) DEFAULT 0 NOT NULL,  /* Last modified timestamp */
  deleted VARCHAR(7) DEFAULT 'FALSE',       /* Is this entry deleted (tombstone) */
  FOREIGN KEY(aceUID) REFERENCES PolicyDb_Ace(aceUID),
  FOREIGN KEY(packageUID) REFERENCES PolicyDb_Package(packageUID),
  PRIMARY KEY(userDataPK));

/* ACE Master policy set */
CREATE TABLE PolicyDb_RuntimePolicy (
  aceUID VARCHAR(128),                      /* The ACE it belongs to. */
  policyVersion INTEGER,                 /* Version of the RT Policy for this ACE */
```

```
  clientPolicyData VARCHAR(2000),           /* Runtime policy for the guest OS */
  clientPolicyDataExtKey VARCHAR(128),     /* If too long store in LongField table */
  hostPolicyData VARCHAR(2000),             /* Runtime policy for the host OS (NQ) */
  hostPolicyDataExtKey VARCHAR(128),       /* If too long store in LongField table */
  expirationType INTEGER NOT NULL,          /* Expiration Type (enum) */
  expValue_1 VARCHAR(21) NOT NULL,          /* Expiration value (depends on type) */
  expValue_2 VARCHAR(21) NOT NULL,          /* Expiration value (depends on type) */
  cacheLifetime VARCHAR(21) NOT NULL,       /* How long could work without server */
  rtpInstType INTEGER NOT NULL,        /* Instantiation authentication check type */
  rtpAuthType INTEGER NOT NULL,             /* Runtime authentication check type */
  rtpUseInstanceLimit VARCHAR(7)
     DEFAULT 'FALSE' NOT NULL,        /* Limit number of instances for this ACE? */
  rtpInstanceLimit INTEGER NOT NULL,        /* Max no. of ACE instances allowed */
  rtpUsePerUserInstanceLimit VARCHAR(7)
     DEFAULT 'FALSE' NOT NULL,              /* Limit number of instances per user? */
  rtpPerUserInstanceLimit INTEGER NOT NULL, /* Max no. of ACE instances per user */
  copyPolicy INTEGER DEFAULT 0 NOT NULL,    /* Behavior if VM instance is copied */
  published VARCHAR(7) DEFAULT 'FALSE' NOT NULL,/* Policy published (update locked)*/
  rtpTsCreated VARCHAR(21) DEFAULT 0 NOT NULL,   /* Creation timestamp */
  rtpTsLastModified VARCHAR(21) DEFAULT 0 NOT NULL,  /* Last modified timestamp */
  deleted VARCHAR(7) DEFAULT 'FALSE',       /* Is this entry deleted (tombstone) */
  PRIMARY KEY (aceUID, policyVersion),
  FOREIGN KEY(aceUID) REFERENCES PolicyDb_Ace(aceUID));

/* ACE Management Server info - reserved for future use */
CREATE TABLE PolicyDb_AcescServer (
  serverHostname VARCHAR(128),              /* Host name of the server computer */
  serverPort INTEGER,                  /* TCP port number server is listening on */
  secure VARCHAR(7) DEFAULT 'FALSE' NOT NULL,  /* Whether HTTPS is enabled */
  sslCertificateExtKey VARCHAR(128),        /* SSL Certificate data, key to stored */
                                            /* in LongField table */
  sslCertificateChainExtKey VARCHAR(128),   /* SSL Certificate Chain data, key to */
                                            /* stored in LongField table */
  PRIMARY KEY (serverHostname, serverPort));

/* Audit Event Log Event Types lookup table */
CREATE TABLE PolicyDb_EventType (
  eventType INTEGER,                        /* Event Type code (PK) */
  eventMessage VARCHAR(1024),              /* Printable message for this event type */
  eventCategory INTEGER,                    /* Event Category code */
  eventCategoryName VARCHAR(128),           /* Event Category printable name */
  eventLogLevel INTEGER,                    /* Event Log Level */
  PRIMARY KEY (eventType));

/* Audit Event Log data */
CREATE TABLE PolicyDb_Event (
  eventUID INTEGER,                      /* Primary key of the table (sequential) */
  eventTs VARCHAR(21),                  /* Timestamp of the event creation in uSec */
  loginName VARCHAR(128),                   /* Login user name of the actor */
  aceUID VARCHAR(128),                      /* UID of the ACE affected by event */
```

```
packageUID VARCHAR(128),                /* UID of the package affected by event */
instanceUID VARCHAR(128),              /* UID of the instance affected by event */
policyVersion INTEGER,              /* Version of ACE policy affected by event  */
eventCategory INTEGER,              /* Event Category as defined in EventType   */
eventType INTEGER,                      /* Event Type as defined in EventType */
sessionID VARCHAR(128),                 /* Ace Server Session ID */
clientIP VARCHAR(128),             /* IP Address of the client machine (resvd) */
serverIP VARCHAR(128),             /* IP Address of the Ace Server (reserved)  */
turnaroundTime VARCHAR(21),             /* Server-side execution time in ms */
handlerName VARCHAR(128),             /* Name of the ClientLib handler (debug) */
returnCodeText VARCHAR(128),         /* Text error code returned to the client */
messageParams VARCHAR(1024),            /* Tab separated list of event data */
prevEventUID INTEGER UNIQUE,            /* UID of the previous recorded event */
eventSignature VARCHAR(128),        /* Event signature, signed with server key  */
FOREIGN KEY(eventType) REFERENCES PolicyDb_EventType(eventType),
FOREIGN KEY(prevEventUID) REFERENCES PolicyDb_Event(eventUID),
PRIMARY KEY (eventUID));
```

Note the following about the database schema:

- A few tables with internal system information and indexes are not listed.
- Boolean values are stored as strings with TRUE or FALSE value.
- Timestamps are stored as decimal 64-bit number strings showing the number of microseconds from 12:00AM 01/01/1970.
- Other dates and times are stored as decimal strings showing the number of seconds from 12:00AM 01/01/1970.
- ACE, Package, Instance, Access, and UserData records are never deleted from the database, but rather marked as deleted with the deleted field set to TRUE, so that the previous information can be inspected for audit purposes.
- The guest and host operating system portions of the ACE policy set are stored in the PolicyDb_RuntimePolicy table in respective fields as strings, if their length is less than 2000 bytes. If the policy component exceeds 2000 bytes, the string is split in 2000-byte chunks and stored in the PolicyDb_LongField table. In this case, the value for the respective ExtKey field in the RuntimePolicy table contains the foreign key pointing to the corresponding series of strings in the LongField table (see the notes in the table definition).

Querying the Audit Event Log Data

You can create an audit trail for all transactions that are performed by the server by using the ACE Serving Component. This system can be used by administrators to track usage, security breaches, policy errors, performance, and so on.

The ACE Server Component Event Logging infrastructure is flexible enough to provide detailed logging when necessary, without overwhelming the system by slowing performance.

The Event Logging mechanism captures enough information to answer the questions like these:

- Who activated an instance?
- When was an instance activated?
- Who revoked an instance?
- Who turned off copy protection policy?
- What changes to policy were made on a particular date?
- Who is failing to authenticate?

The mechanism does not necessarily answer these questions directly, but provides enough data so that an administrator can view event logs and find answers to those questions. The data being logged meets the following requirements:

- Provides details of each transaction served.
- Centralizes the gathering of event log data when multiple servers are used.
- Provides a means for administrators to select which type of transactions are logged.
- Configurable to provide more or fewer logs when necessary.

Some of this audit trail is already visible through other features of the product. For example, the instance viewer displays the date of the last policy get operation, or the expiration date, and so on. The event logging mechanism can answer more difficult questions, such as which administrator made which policy changes, which administrator revoked an instance, which administrator deleted an ACE.

Table A-1 describes the data that is stored in a log entry.

Table A-1. Log Entry Data

Data	Description
Audit log event ID (PK)	An incrementing integer
Log timestamp	In microseconds from 12:00 a.m. 01/01/1970, stored as a decimal string
Login user name	
Affected ACE UID (FK)	

Table A-1. Log Entry Data

Data	Description
Affected package UID (FK)	
Affected instance UID (FK)	
Affected Policy Set Version	
Event category	Auth, AceAdmin, PkgAdmin, PolicyAdmin, InstAdmin
Event type code (FK)	References PolicyDb_EventType table
Session ID	Debug
Incoming IP address	Reserved for future use.
Server IP Address	Reserved for future use.
Operation turnaround time	Time spent in server in ms
Operation handler name (debug)	
Return code text	Success, failure, specific error
Message parameters	Tab-separated list
Previous event UUID to prevent unauthorized record deletion or insertion	Log integrity
Event record hash with a server key to reveal modification of the record	Log integrity

ACE, package, and instance UIDs and policy version provide “coordinates” of the log event in the space of ACE Server objects. They help link the event with the state of the system. By using database query tools such as Crystal Reports, an administrator can find all ACE administration events that affected a particular ACE from its creation until its deletion.

Not all coordinates are present for all events. For example, if a package expiration date update is logged, the instance UID field is not set, because all instances within the package are affected.

If immutable data is stored permanently elsewhere in the database, it is not duplicated in the log entry. For example, when a new policy is published, the complete policy text is not included in the log entry, but rather reference its version number, so that the complete data of the event can be reconstructed from PolicyDb_ RuntimePolicy and PolicyDb_Access tables if necessary.

NOTE ACE Server does not log sensitive data like passwords or encryption keys.

The event type code is associated with a lookup table `PolicyDb_EventType`, which contains a text message template for each type of event, category, and log level of the event. The message can contain parameter placeholders `%s`, in which case the message parameters field in the log entry contains a tab-delimited list of values for these parameters. For example, an instance administration event with type = 4110 has the following message:

```
4110 –> "Instance Set Guest Info requested, IP address = %s, MAC
address %s, configuration message \"%s\", machine name \"%s\",
configuration status %s"
```

In this example, the **Message Parameters** field shows

```
10.17.0.3     00:0C:29:1A:2B:3C       OK    ACETest       0
```

The resulting parameters replace the `%s` placeholders in the message template.

ACE Server event logging contains an experimental tamper evidence feature. Every record in the event log (except the first one) must have a unique reference to the previous event, further enforced by the database foreign key and unique constraint. Each successive record has a unique ID incremented by 1, so missing records are immediately evident. If a user with direct access to the database changes, adds, or removes some records, the user must change either the previous event pointer or other data in the remaining event records. Data within every record is hashed together with a server key, and is stored in the eventSignature field.

For more information about event categories, configuring levels of event logging for each category, and purging old events to keep the table size in check, see the Logging Page section of "Using the ACE Management Server Setup Application" on page 40.

Glossary

ACE instances
The virtual machines that ACE administrators create, associate to virtual rights management (VRM) policies, and then package for deployment to users. In short form, an ACE instance is an ACE.

ACE Management Server
A server that can optionally be installed and used by the ACE administrator for activating and tracking ACE instances and for hosting dynamic policies for ACE instances.

ACE-enabled virtual machine
A virtual machine template created by the ACE administrator. The virtual machine can be configured with various policies and devices and deployment settings and then used as the basis for creating any number of packages to be sent to ACE users.

activation
A step in ACE instance setup that includes package protection and setting up the ACE instance's runtime authentication policy. The successful completion of activation makes the packaged virtual machine, with its policies and other settings, into an ACE instance. The activation setting in the access control policy determines who can access an installed ACE package and turn it into an ACE instance. See also authentication.

authentication
A step in ACE instance setup that includes instance protection. The successful completion of the authentication step allows the user to run the instance. See also activation.

Beta

bridged networking
A type of network connection between an ACE instance and the rest of the world. Under bridged networking, an ACE instance appears as an additional computer on the same physical Ethernet network as the host. See also host-only networking.

configuration
See Virtual machine configuration file.

full screen mode
A display mode in which the ACE instance's display fills the entire screen.

guest operating system
An operating system that runs inside an ACE instance. See also host operating system.

host computer
The physical computer on which the VMware Player software is installed. It hosts the ACE instances.

host-only networking
A type of network connection between an ACE instance and the host. Under host-only networking, an ACE instance is connected to the host on a private network, which normally is not visible outside the host. Multiple virtual machines configured with host-only networking on the same host are on the same network. See also bridged networking and network address translation (NAT).

host operating system
An operating system that runs on the host machine. See also guest operating system.

hot fix
An installable file that resets a user's password, renews an expired virtual machine or allows a cop-protected virtual machine to run from a new location.

instance customization
The act of customizing an ACE instance, thus making it unique from all other instances. The instance customization process automates the actions of the Microsoft sysprep utility. It also provides the ACE administrator with features needed to set up an automated remote domain join process of the ACE instance to a company VPN network.

Beta

live copy of policies

The currently deployed policy set. The active ACE instances on the ACE users' machines use this set.

managed ACE instance

An ACE instance that is managed by an ACE Management Server. See also ACE Management Server.

network address translation (NAT)

A type of network connection that allows you to connect your ACE instances to an external network when you have only one IP network address, and that address is used by the host computer. If you use NAT, your ACE instance does not have its own IP address on the external network. Instead, a separate private network is set up on the host computer. Your ACE instance gets an address on that network from the VMware virtual DHCP server. The VMware NAT device passes network data between one or more ACE instances and the external network. It identifies incoming data packets intended for each ACE instance and sends them to the correct destination.

network access

Policies that give you fine-grained and flexible control over the network access you provide to users of your ACE instances. Using a packet filtering firewall, the network access feature of ACE 2 lets you specify exactly which machines or subnets an ACE instance or its host system may access.

package

An installable bundle for distribution to users. A full package includes an ACE-enabled virtual machine configuration file, virtual disk files, and policies; package installer; and resources files for the ACE-enabled virtual machine. It also includes the VMware Player application used to run ACE instances.

deployment settings

A set of rules and settings associated with a package, such as Instance Customization settings. These settings cannot be changed after packaging. The only way to change deployment settings is to create a new package.

Pocket ACE

An ACE feature that allows the ACE administrator to distribute an ACE instance on a removable device such as a USB key, Apple iPod mobile digital device, or portable hard drive. The user of a Pocket ACE instance can plug the device into a host computer, run the instance, save data from the session and close it, and then

Beta

unplug the device. The user can then take the instance to another host computer and use it in that new location.

policy
A policy controls the capabilities of an ACE instance. Policies are set in the policy editor. See also live copy of policies, working copy of policies, and publish.

preview
An operating and viewing mode that an administrator can use to preview the ACE instance as it will run on the user's machine. The administrator can use this feature to see the effects of policy and configuration settings without having to go through the packaging and deployment steps. The preview mode displays the working copy of the policies. See also working copy of policies.

publish
To publish policies (applies only to managed ACE instances) is to make those policies part of the live copy of the policy set. Publishing copies the working copy of the policies over to the live copy. See also policy, live copy of policies, and working copy of policies.

resume
Return an ACE instance to operation from its suspended state. When you resume a suspended instance, all applications are in the same state they were when the instance was suspended. See also suspend.

snapshot
A snapshot preserves the ACE instance (or ACE-enabled virtual machine) just as it was when you took the snapshot—the state of the data on all the ACE instance's disks and whether the instance was powered on, powered off or suspended.

standalone ACE instance
An ACE instance that is not managed by an ACE Management Server. Any changes to its policies or other settings are made by the administrator's distribution of updates to the user.

suspend
Save the current state of a running ACE instance. To return a suspended ACE instance to operation, use the resume feature. See also resume.

virtual disk
A file or set of files, usually on the host file system, that appears as a physical disk drive to a guest operating system. These files can be on the host machine or on a

Beta

remote file system. When you configure an ACE-enabled virtual machine with a virtual disk, you can install a new operating system into the disk file without the need to repartition a physical disk or reboot the host.

virtual machine
A virtualized x86 PC environment in which a guest operating system and associated application software can run. The managed virtual machine that has policies and other settings associated with it is known as an ACE instance. See also ACE instances.

virtual machine configuration
The specification of what virtual devices (disks, memory size, etc.) are present in a virtual machine (an ACE instance) and how they are mapped to host files and devices.

Virtual machine configuration file
A file, with file extension .vmx, containing an ACE instance configuration. It is used by VMware Player to identify and run a specific ACE instance. See also ACE instances, ACE-enabled virtual machine.

virtual machine settings editor
A point-and-click editor used to view and modify the virtual machine settings of an ACE-enabled virtual machine. You can launch it from the **VM** menu.

Virtual Network Editor
A point-and-click editor used to view and modify the networking settings for the virtual networks created by ACE 2. You can launch it from the **Edit** menu.

VMware Player
A simple application that allows an user to run an ACE instance.

Workstation
The program used by the administrator to create and deploy and update ACE packages and manage ACE instances. Formerly named "VMware ACE Manager" or "VMware Workstation ACE Edition."

VMware Tools
A suite of utilities and drivers that enhances the performance and functionality of your guest operating system. Key features of VMware Tools include some or all of the following, depending on your guest operating system: an SVGA driver, a mouse driver, the VMware Tools control page, and support for such features as shared folders, shrinking virtual disks, time synchronization with the host,

Beta

VMware Tools scripts, and connecting and disconnecting devices while the ACE instance is running.

working copy of policies

The policy that the ACE administrator uses to make and try out policy changes. For managed ACE-enabled virtual machines, the working copy contains "unpublished" policies. For standalone masters, the working copy contains policies that have not yet been packaged or distributed. Manipulating the working copy for a managed ACE-enabled virtual machine does not affect any existing instances associated with that master.

Beta

Index

A

ACE instance
- on Linux host, fixing server connection problem **48**
- reactivating and deactivating from the instance view **59**

ACE Management Server
- Active Directory integration **23**
- caution, when installing **26**
- changing port assignment **48**
- components **23**
- configuring **34**
- creating Active Directory user and group for **34**
- database backup **24**
- database schema **63**
- default port assignments **26**
- description **73**
- embedded database **23**
- external database option **23**
- features **20**
- fixing connection problem with ACE instance on Linux host **48**
- hardware requirements **9**
- installing **25**
- installing on Linux system **27**
- installing on Windows system **26**
- installment options **26**
- instance view **55**
- licensing **34**
- logging on **47**
- opening Instance View with Connect to ACE Management Server command **62**
- querying the audit event log data **63**
- serial number **34**
- setting name **26**
- stopping and starting manually **46**
- using **48**

activation, defined **73**

Active Directory
- creating group for use with ACE Management Server **34**
- creating user for use with ACE Management Server **34**
- integration with ACE Management Server **23**
- logon options, ACE Management Server **47**

audit event log data, querying **68**

authentication, defined **73**

B

bridged networking, defined **74**

C

caution
- check server name when installing ACE Management Server **26**

certificates, setting up **31**

change the copy protection ID **53**

clock synchronization (note) **21**

column headings, sorting by **52**

configuring
- ACE Management Servers **34**

Beta

virtual machines, defined **77**
Connect to ACE Management Server command **62**
copy protection, changing the ID for **53**
custom fields in Instance View **58**

D

database for ACE Management Server **23**
database, backup **24**
database, external **23**
deactivate or reactivate an instance **52**
deactivating ACE instances from the instance view **59**
details for an instance, viewing **53**
disks, virtual **76**

E

event logging **46**
expiration date for instance, resetting **53**

F

full screen
mode, defined **74**

G

guest operating system
defined **74**

H

Help Desk
advanced instance queries **50**
Instance Details page **52**
Instances page **50**
using **49**
host computer, defined **74**
host operating system, defined **74**
host-only networking
defined **74**
hot fix
defined **74**

I

installing
ACE Management Server **25**
instance customization
defined **74**
Instance Details page
accessing from the Instances page **52**
using **52**
instance queries **50**, **56**
Instance View
advanced instance queries **56**
custom fields **58**
deactivating ACE instance from **59**
description **55**
opening with Connect to ACE Management Server command **62**
reactivating ACE instance from **59**
Instances page **50**

K

knowledge base
accessing **8**

L

LDAP
See Active Directory
licensing, ACE Management Server **34**
logging events **46**
logging on to the ACE Management Server **47**

M

managed ACE instance, defined **75**
mode, full screen **74**

Beta

N

NAT
- defined **75**

network
- bridged networking, defined **74**
- host-only **74**
- NAT, defined **75**
- Virtual Network Editor **77**

network access, viewing details for **54**
network address translation, defined **75**
network quarantine
- defined **75**

O

operating system
- guest, defined **74**
- host, defined **74**

P

package
- defined **75**

package settings
- description **75**

password
- resetting **53**

policy, defined **76**
port assignments, default **26**
port for ACE Management Server **48**
preview, defined **76**
publish, defined **76**

Q

quarantine
- network, defined **75**

R

reactivate or deactivate an instance **52**
reactivating ACE instances from the instance view **59**
reset the expiration date **53**
reset the password for an instance **53**
resume, defined **76**

S

searching for instances in Help Desk **50**
searching for instances in Instance View **56**
security, SSL **30**
server name, setting for ACE Management Server **26**
setting
- server name for ACE Management Server **26**

snapshot
- defined **76**

sort instances **52**
SQLite database for ACE Management server **23**
SSL certification, using **30**
SSL protocol, using **30**
standalone ACE instance, defined **76**
stopping and starting the Apache service manually **46**
suspend, defined **76**

T

technical support resources **7**
troubleshooting
- Help Desk Web application **49**

U

user groups, accessing **8**
using the ACE Management Server **48**

V

view details for an instance **53**
view network access details **54**
viewing instances managed by an ACE Management Server **56**

Beta

virtual disk
defined **76**
virtual machine
defined **77**
settings editor, defined **77**
Virtual Network Editor **77**
VMware ACE Management Server
database schema script **64**
VMware community forums, accessing **8**
VMware Player
defined **77**
fixing ACE Server connection problem on Linux host **48**
VMware Tools
defined **77**

W

Workstation ACE Edition
defined **77**

Beta